From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Daily Cyber Report - 2011-12-28
Date:	Wednesday, December 28, 2011 10:46:40 AM
Attachments:	DHS_Cyber_Report_2011-12-28.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 28 December 2011 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6) .

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise Daily Cyber Report
28 December 2011

CRITICAL INFRASTRUCTURE PROTECTION:

- **Embedded Attacks And Emerging Targets To Dominate 2012 Security Landscape:** [McAfee's] 2012 Threat Predictions Report said that attacks on industrial systems and embedded hardware will continue as utility companies increasingly use network-connected systems to control infrastructure. Dave Marcus, head of research and communications at McAfee Labs, told V3 that the danger of attack on industrial systems could be compounded as hacktivist groups such as Anonymous shift to political protests. … McAfee also predicts an increase in the use of phoney or compromised digital certificates, such as the Diginotar breach, to spread malware and launch targeted attacks. … McAfee believes that commercial spam from mailing lists will become more prevalent as companies advertise via email, but that malware and phishing attacks will decline. [HSEC-1.1; Date: 28 December 2011; Source: http://www.v3.co.uk/v3-uk/news/2134518/embedded-attacks-emerging-targets-dominate-2012-security-landscape]

- **Cyber Threat To Power Grid Puts Utility Investors At Risk:** The electric-utility industry's concerns about cyber security have escalated sufficiently for several investor-owned utilities to include cyber-attacks as a material risk factor in recent filings with the U.S. Securities and Exchange Commission. In November, Consolidated Edison of New York, a large electric and gas utilities serving customers in New York City and Westchester County, included cyber-attacks as a risk factor that could affect investors' quarterly report (10-Q) for the first time. … [T]he grid's vulnerabilities to hackers are expanding more rapidly than the prophylactic measures needed to protect the grid from attack. This grim conclusion is among the many grim findings of a major new study on the "Future of the Electric Grid" by researchers at the Massachusetts Institute of Technology. [HSEC-1.1; Date: 27 December 2011; Source: http://www.forbes.com/sites/williampentland/2011/12/27/cyber-threat-to-power-grid-puts-utility-investors-at-risk/]

INFORMATION SYSTEMS BREACHES:

- **Hackers Vow To Publish Emails Stolen From Stratfor:** Hackers affiliated with the Anonymous group [Antisec] said they are getting ready to publish emails stolen from private intelligence analysis firm Strategic Forecasting Inc.… Antisec has already published what it claims are the names of thousands of corporate and government customers, as well as email addresses, passwords and credit card numbers of individual subscribers to its services. Customers on the list published by Antisec include Bank of America, Exxon Mobil Corp, Goldman Sachs & Co, Interpol, Thomson Reuters, the U.S. military and the United Nations. … Anonymous said that the emails the hackers intended to publish would be more sensitive. … The group said it would release those emails once it had finished formatting them for distribution and prepared more than 9,000 "mirrored" copies. [HSEC-1.10; Date: 27 December 2011; Source: http://www.msnbc.msn.com/id/45799865/ns/technology_and_science-security/]

- **Report Details Extent Of Anonymous Hack On Stratfor:** [I]dentity Finder, a New York-based data loss and identity theft prevention service, today published a report stating that AntiSec has so far released personal information obtained in the hack for Stratfor subscribers with first names beginning with A through M. The rest of the alphabet, along with what AntiSec claims are copies of 2.7 million e-mails, are expected to be released in upcoming days. Documents from the hack posted to date by both Anonymous and AntiSec, according to Identity Finder, include: … 50,277 unique credit card numbers, of which 9,651 are not expired[;] 86,594 e-mail addresses, of which 47,680 are unique[;] 27,537 phone numbers, of which 25,680 are unique[; and] 44,188 encrypted passwords, of which roughly 50 percent could be easily cracked. [HSEC-1.10; Date: 27 December 2011; Source: http://news.cnet.com/8301-1009_3-57348995-83/]

- **Anonymous Hacks SpecialForces.com, Posts Passwords And Credit Card Data:** Members of the hacker collective Anonymous claim they have stolen about 14,000 user passwords and 8,000 credit card numbers from SpecialForces.com, a military and law enforcement equipment retailer. The data breach occurred several months ago, according to Anonymous, but the group only now decided to post the data online. The purloined password list had reportedly been posted online several weeks ago as well. A Twitter account associated with Anonymous has posted a screenshot of an e-mail from SpecialForces.com dated Dec. 15 admitting to the data breach. … Anonymous members were apparently motivated to attack SpecialForces.com because, the hackers believe, the site's customers are largely "military and law enforcement affiliated individuals." [HSEC-1.10; Date: 28 December 2011; Source: http://www.pcworld.com/article/247072/]

CYBERTERRORISM & CYBERWARFARE:

- **South Korean Military Lowers Cyber Alert To Normal Level:** South Korea's military lowered its cyber alert level, which was raised after the death of North Korea's Kim Jong Il, to the normal level, said a spokesman at the joint chiefs of staff, who declined to be named, citing military policy. The level is back to "infocon 5," said the spokesman.... South Korea's military and civilian government raised their cyber alert levels after the death of the North Korean, whose regime has been linked with online attacks against its neighbor. [HSEC-1.1; Date: 27 December 2011; Source: http://www.businessweek.com/news/2011-12-27/south-korean-military-lowers-cyber-alert-to-normal-level.html]

VULNERABILITIES:

- **WiFi Protected Setup Flaw Can Lead To Compromise Of Router PINs:** The US-CERT is warning about a vulnerability in the WiFi Protected Setup standard that reduces the number of attempts it would take an attacker to brute-force the PIN for a wireless router's setup process. The flaw results in too much information about the PIN being returned to an attacker and makes the PIN quite weak, affecting the security of millions of WiFi routers and access points. WPS is a method for setting up a new wireless router for a home network and it includes a way for users to set up the network via an external or internal registrar. In this method, the standard requires a PIN to be used during the setup phase. The PIN often is printed somewhere on the wireless router or access point. The vulnerability discovered in WPS makes that PIN highly susceptible to brute force attempts. [HSEC-1.1; Date: 27 December 2011; Source: http://threatpost.com/en_us/blogs/wifi-protected-setup-flaw-can-lead-compromise-router-pins-122711]

- **Security Experts Find Defective SMS Trojan:** Researchers from F-Secure came across a large number of Trojans that were initially designed to seamlessly send SMSs to premium rate numbers with the purpose of filling the pockets of the cybercriminals who launch them. The only problem is that the latest series of these malicious apps contain a bug in the source code that makes them crash. Identified as Trojan:Android/RuFailedSMS.A, the applications request the same permissions as most of these Trojans do, including permission to access storage, network communication, services that cost money and phone calls. … Programmed to target users from Russia, Belarus, Kazakhstan and Azerbaijan, hundreds of these malicious apps were found on third-party Android markets. Even though at the moment none of the applications that hide RuFailedSMS are working, this can change at any minute. [HSEC-1.1; Date: 28 December 2011; Source: http://news.softpedia.com/news/Security-Experts-Find-Defective-SMS-Trojan-243369.shtml]

- **360Buy.com Security Risks Exposed:** China's leading online retailer 360buy.com contains security flaws that can easily lead to user data leaks, the internet vulnerability reporting platform Wooyun said on Tuesday. According to Wooyun, under 360buy.com's current user permission control system, some users can access the private information of all users, including names, addresses, email addresses and phone numbers, after logging in to the site. 360buy.com has thus far denied the existence of any security flaws. However, Li Daxue, vice president of the online retailer's information department, said his company is currently examining its system for any vulnerability. [HSEC-1.1; Date: 28 December 2011; Source: http://www.china.org.cn/business/2011-12/28/content_24273634.htm]

GENERAL CYBER/ELECTRONIC CRIME:

- **French MP Valerie Boyer's Website Hacked for Genocide Denial Bill:** A Turkish hacker collective defaced the personal website of Valerie Boyer (valerie-boyer.fr), a member of the French parliament, as a result of the fact that she authored a bill that fines and imprisons anyone who denies genocide acts. According to The Hacker News, Boyer called the police after she and her family received numerous death threats. The attack on Boyer's site comes after a few days ago the French National Assembly passed a bill that refers to the criminalization of anyone who publicly denies the Armenian Genocide. [HSEC-1.10; Date: 27 December 2011; Source: http://news.softpedia.com/news/French-MP-Valerie-Boyer-s-Website-Hacked-for-Genocide-Denial-Bill-243126.shtml]

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Daily Cyber Report - 2011-12-29
Date:	Thursday, December 29, 2011 9:34:25 AM
Attachments:	DHS_Cyber_Report_2011-12-29.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 29 December 2011 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise Daily Cyber Report
29 December 2011

CRITICAL INFRASTRUCTURE PROTECTION:

- **Hackers Could Shut Down Train Lines:** Hackers who have shut down websites by overwhelming them with Web traffic could use the same approach to shut down the computers that control train switching systems, a security expert said at a hacking conference in Berlin. Stefan Katzenbeisser, professor at Technische Universität Darmstadt in Germany, said switching systems were at risk of "denial of service" attacks, which could cause long disruptions to rail services. … Katzenbeisser said GSM-R, a mobile technology used for trains, is more secure than the usual GSM, used in phones, against which security experts showed a new attack at the convention. [HSEC-1.1; Date: 28 December 2011; Source: http://www.reuters.com/article/2011/12/28/us-trains-security-idUSTRE7BR0C520111228]
- **Buffer Overflow Vulnerability Identified In Sielco Sistemi SCADA System:** The US Department of Homeland Security (DHS) is warning about a buffer overflow vulnerability in the Sielco Sistemi Winlog application used to control industrial systems. A hacker could exploit this vulnerability, identified by independent researcher Paul Davis, to carry out an arbitrary code execution or program crash, according to the advisory issued by the DHS Industrial Control Systems Cyber Emergency Response Team. … Affected products include Winlog Lite and Winlog PRO versions older than Version 2.07.09. ... Sielco Sistemi has produced a new release that mitigates the vulnerability, which Davis has validated as resolving the issue. [HSEC-1.1; Date: 28 December 2011; Source: http://www.infosecurity-magazine.com/view/22865/]
- **SCADA And PLC Vulnerabilities In Correctional Facilities:** Many prisons and jails use SCADA systems with PLCs to open and close doors. Using original and publicly available exploits along with evaluating vulnerabilities in electronic and physical security designs, researchers discovered significant vulnerabilities in PLCs used in correctional facilities by being able to remotely flip the switches to "open" or "locked closed" on cell doors and gates. [HSEC-1.1; Date: 28 December 2011; Source: http://www.net-security.org/secworld.php?id=12145]

INFORMATION SYSTEMS BREACHES:

- **Specialforces.com Says Hack Of Customer Data Is Six Months Old:** [I]n a message posted on the Web site hacktalk.net, an individual claiming to represent Anonymous, linked the attack [on SpecialForces.com] to the hack earlier this week of Stratfor and said it was part of a "week long celebration of wreaking utter havoc on global financial systems, militaries, and governments." … An employee at Specialforces.com acknowledged that a breach took place, but said it happened more than six months ago and suggested the group was recycling old news to promote its image. [HSC-1.10; Date: 28 December 2011; Source: http://threatpost.com/en_us/blogs/specialforcescom-says-hack-customer-data-six-months-old-122811]
- **Whoops! Cancellation E-Mail Meant For 300 Rattles 8 Million New York Times Subscribers:** An errant e-mail campaign has rattled subscribers to the New York Times with false cancellation notices. The e-mail blast meant for 300 subscribers was instead sent to 8 million current subscribers, raising speculation that the paper suffered a data breach. The e-mail, which was widely received, led to confusion and complaints online, as Times subscribers, and non-subscribers reported receiving it. A spokesperson for the New York Times did not immediately respond to a request for comment from Threatpost. However, New York Times corporate media reporter Amy Chozick…used her Twitter account on Wednesday to report that the email was the result of an error, not a hack. [HSEC-1.1; Date: 28 December 2011; Source: http://threatpost.com/en_us/blogs/whoops-cancellation-e-mail-meant-300-rattles-8-million-new-york-times-subscribers-122811]

CYBERTERRORISM & CYBERWARFARE:

- **Stuxnet Weapon Has At Least 4 Cousins:** The Stuxnet virus that last year damaged Iran's nuclear program was likely one of at least five cyber weapons developed on a single platform whose roots trace back to 2007, according to new research from Russian computer security firm Kaspersky Lab. … Kaspersky's director of global research & analysis, Costin Raiu, told Reuters on Wednesday that his team has gathered evidence that shows the same platform that was used to build Stuxnet and Duqu was also used to create at least three other pieces of malware. Raiu said the platform is comprised of a group of compatible software modules designed to fit together, each with different functions. Its developers can build new cyber weapons by simply adding and removing modules. … Kaspersky named the platform "Tilded" because many of the files in Duqu and Stuxnet have names beginning with the tilde symbol "~" and the letter "d." [HSEC-1.8; Date: 28 December 2011; Source: http://www.msnbc.msn.com/id/45809884/]

VULNERABILITIES:

- **Huge Portions Of The Web Vulnerable To Hashing Denial-Of-Service Attack:** Researchers have shown how a flaw that is common to most popular Web programming languages can be used to launch denial-of-service attacks by exploiting hash tables. Announced publicly on Wednesday at the Chaos Communication Congress event in Germany, the flaw affects a long list of technologies, including PHP, ASP.NET, Java, Python, Ruby, Apache Tomcat, Apache Geronimo, Jetty, and Glassfish, as well as Google's open source JavaScript engine V8. The vendors and developers behind these technologies are working to close the vulnerability…. On Wednesday, Microsoft published its own security advisory, recommending that all ASP.NET website admins evaluate their risk and implement a workaround that Microsoft has posted while it works on a patch to be released in a future security update. [HSEC-1.1; Date: 28 December 2011; Source: http://arstechnica.com/business/news/2011/12/huge-portions-of-web-vulnerable-to-hashing-denial-of-service-attack.ars]
- **Microsoft Releases Out-Of-Band Security Bulletin For ASP.NET/IIS On All Windows Versions:** On December 29, 2011, at 10:00 AM Pacific Time Microsoft will release an out-of-band security update to address a critical security flaw found in ASP.NET, that affects all supported versions of the .NET framework, which could allow for an unauthenticated denial-of-service (DoS) attack on servers that serve ASP.NET webpages. These attacks that exploit hash tables, known as hash collision attacks, are not specific to Microsoft technologies, but other web service software providers may be affected. … While the information is out there and hackers could take advantage of it, Microsoft is unaware of any active attacks that rely on this flaw. [HSEC-1.1; Date: 29 December 2011; Source: http://news.softpedia.com/news/Microsoft-to-Release-Out-of-Band-Security-Bulletin-for-All-Windows-Versions-243473.shtml]

GENERAL CYBER/ELECTRONIC CRIME:

- **Aggressive Phishing Attack Targets Military Personnel:** The U.S. military received an unwanted present this Christmas holiday season in the form of an "aggressive" phishing attack that's been making the rounds of .mil email accounts, according to the Army. There are several attacks making the rounds, the most notable coming in the form of an email with the subject line "Deposit Posted" that appears to be from USAA…. Other attacks have targeted U.S. military installations and defense facilities with emails that appear to come from senior officers or military authority figures. Those emails also request that the recipient download and install software that's depicted as a "critical security measure that must be immediately deployed," according to the Army. But rather than providing security, the software instead is either a Trojan Horse that can destroy systems and networks or data-mining software that can provide hackers with unauthorized access to information behind the firewall. [HSEC-1.10; Date: 28 December 2011; Source: http://www.informationweek.com/news/government/security/232301104]
- **Koobface Gang Redirects Web Traffic To Fuel Pay-Per-Click Profits:** The group behind the Koobface is back, and they are reinventing themselves to take advantage of pay-per-click advertising, according to Trend Micro. The Koobface developers updated their botnet framework with a "sophisticated" traffic-direction system (TDS) that handles traffic referenced to their affiliate sites, Trend Micro researchers reported. They have also added components to help increase the amount of Internet traffic, "which translates to even bigger profit", wrote Jonell Baltazar, senior threat researcher at Trend Micro, on the company's TrendLabs Malware Blog. It appears that the TDS may also be offered as a service to others…. [HSEC-1.8; Date: 28 December 2011; Source: http://www.techweekeurope.co.uk/news/koobface-gang-redirects-web-traffic-to-fuel-pay-per-click-profits-51576]

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Daily Cyber Report - 2012-01-06
Date:	Friday, January 06, 2012 9:43:39 AM
Attachments:	DHS_Cyber_Report_2012-01-06.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 06 January 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise Daily Cyber Report
6 January 2012

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- **Anonymous Targets New York Officials And Companies:** Anonymous…has targeted New York's top officials, companies and organizations as part of one of its latest operations. Dubbed Operation Hiroshima, or #OpHiroshima, the New Year's Day document dump was an attempt to "dox," or release revealing information, about a wide range of targets through a variety of internet channels. … New York was not the only area targeted under the widespread doxing operation. The Boston and Oakland police departments were also hit with doc dumps, as were UC Davis, and a range of Washington officials including federal judge Liam O'Grady and FBI Director Robert Mueller. [HSEC-1.10; Date: 5 January 2012; Source: http://newyork.ibtimes.com/articles/277267/20120105/anonymous-targets-new-york-officials-companies-video.htm]

CYBERTERRORISM & CYBERWARFARE:

- **Saudi Hacker Claims Info On 1M Israeli Credit Cards:** The Saudi Arabian hacker who styles himself OxOmar claims that he has details of some one million credit cards belonging to Israelis, mocking the claims of Israeli credit companies that details of only 14 thousand credit cards were stolen in the break-in to Israeli websites. … Today, Omar has published an additional list with details of 11,000 cards, and claims that this is a partial list out of 60,000 cards details of which will be published in full shortly. … Despite earlier denials by security experts that this was a deliberate hacking attack on Israel, there now appears to be no doubt that it is such an attack, as indicated by the hacker's frequent use of the words "Zionist" and "Zionist lobby". [HSEC-1.10; Date: 5 January 2012; Source: http://www.globes.co.il/serveen/globes/docview.asp?did=1000713304]

VULNERABILITIES:

- **New Denial-Of-Service Attack Cripples Web Servers By Reading Slowly:** A researcher today published proof-of-concept code that takes a different spin on the slow HTTP denial-of-service attack simply by dragging out the process of reading the server's response -- ultimately overwhelming it. Sergey Shekyan, senior software engineer with Qualys, also has now added this new so-called Slow Read attack to his open source slowhttptest tool. Slow Read basically sends a legitimate HTTP request and then very slowly reads the response, thus keeping as many open connections as possible and eventually causing a denial-of-service. … Slow HTTP attacks are gaining in popularity among the bad guys as a way to quietly wage a denial-of-service attack because these exploits are relatively easy to perform and require minimal computing resources, and often are tough to detect until it's too late. [HSEC-1.8; Date: 5 January 2012; Source: http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232301367/]

- **Chrome 17 Enters Beta, Improves Speed And Security:** Version 17 of Chrome has been released into the WebKit-based browser's Beta channel. … With version 17, Chrome's Safe Browsing technology has been extended to protect against malicious downloads by analysing executable files, including Windows .exe and .msi files. … The Chrome Team at Google has also updated the browser's Stable channel to version 16.0.912.75, closing three high risk security holes. These include a use-after-free in animation frames, a heap-buffer-overflow in the libxml software library, and a stack-buffer-overflow in glyph handling. [HSEC-1.1; Date: 6 January 2012; Source: http://www.h-online.com/security/news/item/Chrome-17-enters-beta-improves-speed-and-security-1404530.html]

GENERAL CYBER/ELECTRONIC CRIME:

- **Symantec Confirms Source Code Leak In Two Enterprise Security Products:** Symantec late Thursday confirmed that source code used in two of its older enterprise security products was publicly exposed by hackers this week. In a statement, the company said that the compromised code is between four and five years old and does not affect Symantec's consumer-oriented Norton products as had been previously speculated. … Symantec spokesman Cris Paden identified the two affected products as Symantec Endpoint Protection 11.0 and Symantec Antivirus 10.2. … An Indian hacking group calling itself Lords of Dharmaraja had earlier claimed that it had accessed source code for Symantec's Norton AV products. … Comments posted by Yama Tough on Google+ and Pastebin suggest that the Symantec information was accessed from an Indian government server. [HSEC-1.10; Date: 6 January 2012; Source: http://www.computerworld.com/s/article/9223198/]

- **Sony Gets Hacked By Anonymous:** Hacktivist group Anonymous has lived up to his threat to attack Sony over its support for the Stop Online Piracy Act (SOPA) in the US. … The hack hit the Sony Pictures Facebook page and its web site homepage, according to reports and tweets from those involved. Comments were left on the web pages, but have since been removed. The attacks carry the name Op Sony and were noted through the @s3rver_exe Twitter account. … Another account associated with Operation Censor This and both Anonymous and Team Poison under their P0isAnon guise acknowledged the hack. [HSEC-1.10; Date: 6 January 2012; Source: http://www.theinquirer.net/inquirer/news/2135722/sony-hacked-anonymous]

- **ArcelorMittal Hacked By Anonymous, Tons Of Information Leaked:** [Anonymous Belgium]…managed to breach the main website belonging to ArcelorMittal, the largest steel producing company in the world, leaking a large quantity of information from their databases. ArcelorMittal's website…is currently offline while the company's IT department is probably patching up the wholes and assessing the damage caused by the hacktivists. Several cross-site scripting (XSS) and SQL injection vulnerabilities allowed the hackers to breach their website and leak information on their users and administrators. [HSEC-1.10; Date: 6 January 2012; Source: http://news.softpedia.com/news/ArcelorMittal-Hacked-by-Anonymous-Tons-of-Information-Leaked-244898.shtml]

- **Ramnit Worm Goes After Facebook Credentials:** A pervasive worm has expanded its reach to now steal login and password details for Facebook users, warned security vendor Seculert, which found a server holding 45,000 login credentials. The worm, called Ramnit, infects Windows executables, Microsoft Office and HTML files, according to a profile published by Microsoft. … Researchers from Seculert discovered a command-and-control server for the worm and found that it had harvested some 45,000 credentials from Facebook users, mostly in the U.K. and France, according to its blog. … Another security vendor, Trusteer, noted last year that Ramnit appeared to have been modified in order to commit financial fraud, acquiring similar capabilities as the famous Zeus and SpyEye malicious software programs. [HSEC-1.8; Date: 5 January 2012; Source: http://www.computerworld.com/s/article/9223173/Ramnit_worm_goes_after_Facebook_credentials]

- **Pharma Wars: Mr. Srizbi Vs. Mr. Cutwail:** The previous post in this series introduced the world to "Google," an alias chosen by the hacker in charge of the Cutwail spam botnet. Google rented his crime machine to members of SpamIt, an organization that paid spammers to promote rogue Internet pharmacy sites. This made Google a top dog, but also a primary target of rival botmasters selling software to SpamIt, particularly the hacker known as "SPM," the brains behind the infamous Srizbi botnet. Today's Pharma Wars entry highlights that turf battle, and features newly discovered clues about the possible identity of the Srizbi botmaster, including his whereabouts and current occupation. [HSEC-1.2; Date: 5 January 2012; Source: http://krebsonsecurity.com/2012/01/pharma-wars-mr-srizbi-vs-mr-cutwail/]

- **Pastebin Downed By Second DDoS Attack This Week:** For the second time this week, Pastebin.com on Thursday found itself hit by a distributed denial-of-service (DDoS) attack. The site was previously taken offline for a portion of the day on Tuesday, though no motives or culprits for that attack have been named yet. A post to the service's Twitter account…around 1:30 p.m. acknowledged the attack: "Pastebin is under DDOS attack again guys, working on it..." [HSEC-1.10; Date: 5 January 2012; Source: http://threatpost.com/en_us/blogs/pastebin-downed-second-ddos-attack-week-010512]

- **Kim Jong-Il YouTube Video Used To Spread Malware:** ESET researchers from Latin America found a piece of malware being spread with the help of a YouTube video that allegedly presents the death of Kin Jong-il. Unlike other schemes where the clip is actually a fake, in this scenario the video is real, but it displays only a couple of still images, urging users to check out the complete video at a URL displayed in the description. Once the link is clicked, the victim is taken to a blog that allegedly offers movies and TV shows, but almost immediately, a pop-up window advises users to install an add-on called ClickPotato which comes with additional suspicious toolbars. [HSEC-1.8; Date: 5 January 2012; Source: http://news.softpedia.com/news/Kim-Jong-il-YouTube-Video-Used-to-Spread-Malware-244597.shtml]

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Daily Cyber Report - 2012-02-08
Date:	Wednesday, February 08, 2012 10:04:42 AM
Attachments:	DHS_Cyber_Report_2012-02-08.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 08 February 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Cyber Report
8 February 2012

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- **Symantec Expects Anonymous To Publish More Stolen Source Code:** Symantec today confirmed that the pcAnywhere source code published on the Web Monday by hackers who tried to extort $50,000 from the company was legitimate. A company spokesman also said that Symantec expects that the rest of the source code stolen from its network in 2006 will also be made public. Symantec's acknowledgement followed the appearance late Monday of a 1.3GB file on various file-sharing websites, including Pirate Bay, that claimed to be the source code of the pcAnywhere remote-access software. … Also on Monday, an individual or group going by the name "Yama Tough" had published a series of emails on Pastebin that detailed an attempt to extort $50,000 from Symantec. Previously, Yama Tough had claimed responsibility for stealing the source code to pcAnywhere and other Symantec security software. [HSEC-1.10; Date: 7 February 2012; Source: http://www.computerworld.com/s/article/9224039/]

CYBERTERRORISM & CYBERWARFARE:

- **Hackers Group Posts Police Chiefs' Information Online:** The Federal Bureau of Investigation is looking for the people responsible for leaking the home addresses, home phone numbers and cellphone numbers of every police chief in West Virginia, according to the president of a statewide police chiefs organization. William Roper, president of the West Virginia Chiefs of Police Association, said his organization's website was compromised Monday by a group associated with Anonymous, an international hacker group with a stated mission of protecting free speech and fighting anti-piracy laws. The subgroup, which calls itself "CabinCr3w," posted the personal information of more than 156 police officers, including current and retired police chiefs, to a public website. [HSEC-1.10; Date: 7 February 2012; Source: http://wvgazette.com/News/201202070284]

VULNERABILITIES:

- **Trustwave Issued A Man-In-The-Middle Certificate:** Certificate authority Trustwave issued a certificate to a company allowing it to issue valid certificates for any server. This enabled the company to listen in on encrypted traffic sent and received by its staff using services such as Google and Hotmail. Trustwave has since revoked the CA certificate and vowed to refrain from issuing such certificates in future. According to Trustwave, the CA certificate was used in a data loss prevention (DLP) system, intended to prevent confidential information such as company secrets from escaping. The DLP system monitored encrypted connections by acting as a man-in-the-middle, meaning that it tapped into the connection and fooled the browser or email client into thinking it was communicating with the intended server. [HSEC-1.1; Date: 7 February 2012; Source: http://www.h-online.com/security/news/item/Trustwave-issued-a-man-in-the-middle-certificate-1429982.html]

- **Adobe Sets IE As Next Target In Flash Security Work:** Adobe plans to tackle Microsoft's Internet Explorer (IE) in its ongoing work to "sandbox" its popular Flash Player within browsers, Adobe's head of security said today. … "IE has a big chunk of the user base," said Brad Arkin, senior director of security, products and services, in an interview Tuesday. "We want to do what protects the most users the fastest, so we're looking

at how we can tackle sandboxing in IE." … But Akin declined to set a timetable for putting Flash within a sandbox inside IE. "The way that Flash integrates with IE is at a very low level," he said, noting that the two programs frequently share the same memory space. IE also uses an entirely different plug-in infrastructure -- Microsoft's own ActiveX technology -- than other browsers. [HSEC-1.1; Date: 7 February 2012; Source: http://www.computerworld.com/s/article/9224047/]

- **'Offensive Security Research Community Helping Bad Guys':** During a keynote presentation at the Kaspersky security analyst summit, [Adobe security chief Brad Arkin] said the intellectual pursuit of exploiting software vulnerabilities and defeating mitigations is simply providing a roadmap for the bad guys to break into computer systems. "We are involved in a cat-and-mouse game on [the software] engineering side. Every time we come up with something new and build new defenses, it creates incentive for the bad guy to look beyond that," Arkin explained, noting that the white-hat security research community helps cyber-criminals by publishing vulnerabilities, exploits and techniques to bypass security mitigations. … Arkin said that the volume of reported security vulnerabilities is forcing Adobe to respond in a way that may introduce new security defects. [HSEC-1.1; Date: 7 February 2012; Source: http://www.zdnet.com/blog/security/offensive-security-research-community-helping-bad-guys/10228]

- **Crypto Crack Makes Satellite Phones Vulnerable To Eavesdropping:** Cryptographers have cracked the encryption schemes used in a variety of satellite phones, a feat that makes it possible for attackers to surreptitiously monitor data received by vulnerable devices. The research team, from the University of Ruhr in Bochum, Germany, is among the first to analyze the secret encryption algorithms implemented by the European Telecommunications Standards Institute. After reverse engineering phones that use the GMR-1 and GMR-2 standards, the team discovered serious cryptographic weaknesses that allow attackers using a modest PC running open-source software to recover protected communications in less than an hour. [HSEC-1.1; Date: 8 February 2012; Source: http://arstechnica.com/business/news/2012/02/crypto-crack-makes-satellite-phones-vulnerable-to-eavesdropping.ars]

GENERAL CYBER/ELECTRONIC CRIME:

- **Move Over Cybercrims, DDoS Now Protesters' Weapon Of Choice:** Ideological hacktivism has replaced cybercrime as the main motivation behind DDoS attacks, according to a study by Arbor Networks. Up until last year, DDoS attacks were typically financially driven – either for reasons of competition or outright extortion – but the activities of Anonymous and related groups have changed that. The plethora of readily available DDoS attack tools (such as LOIC, a sometime favourite of Anonymous) means that anyone can launch an attack and any business could potentially be targeted. [HSEC-1.5; Date: 8 February 2012; Source: http://www.theregister.co.uk/2012/02/08/ddos_attack_trends/]

- **Attackers Using Fake Google Analytics Code To Redirect Users To Black Hole Exploit Kit:** Injecting malicious code into the HTML used on legitimate Web sites is a key part of the infection lifecycle for many attack crews, and they often disguise and obfuscate their code to make it more difficult to analyze or so it appears to be legitimate code. The latest instance of this technique has seen attackers employing code that is meant to look like Google Analytics snippets, but instead sends victims off to a remote site that's hosting the Black Hole Exploit Kit. Not the desired result. Researchers at Websense discovered the ongoing attack recently, and found that the code being used to hide the fake Google Analytics tags is heavily obfuscated, making analysis quite difficult. [HSEC-1.8; Date: 8 February 2012; Source: http://threatpost.com/en_us/blogs/attackers-using-fake-google-analytics-code-redirect-users-black-hole-exploit-kit-020812]

- **More Bogus Ad-Serving Android Apps Evade Google's Bouncer:** Users searching for games on the official Android Market have lately been heavily targeted by ad-pushing scammers. First it was the fake Temple Run app, and now a string of bogus copies of popular iPhone games supposedly developed by Rovio Mobile Ltd, the developers of the famous Angry Birds game**.** In reality, some of these games are offered by other developers - mostly on Apple's iPhone Apps Store - and some do not even exist, but the scammers are trying to take advantage of the fact that Angry Birds' developer Rovio has become a very well known and trusted name. So how could the scammers register their account under that name? The explanation is very simple: they used a capital "I" instead of a lowercase "L" in "Mobile" and the result was a legitimate looking account. [HSEC-1.1; Date: 8 February 2012; Source: http://www.net-security.org/secworld.php?id=12367]

From: OSINT Branch Mailbox
To: OSINT Branch Mailbox
Subject: DHS-OSE Daily Cyber Report - 2012-03-09
Date: Friday, March 09, 2012 9:23:11 AM
Attachments: DHS_Cyber_Report_2012-03-09.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 09 March 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Cyber Report
9 March 2012

CRITICAL INFRASTRUCTURE PROTECTION:

- **How Anonymous Plans To Use DNS As A Weapon:** After engaging in a recent rash of attacks in retaliation for the takedown of file-sharing site Megaupload, the Anonymous denial of service "cannons" have been firing considerably fewer shells of late. … Disappointed with the current denial of service tools at their disposal, members of Anonymous are working to develop a next-generation attack tool that will, among other options, use DNS itself as a weapon. … The scale and stealthiness of the technique, called DNS amplification, is its main draw for Anonymous. DNS amplification hijacks an integral part of the Internet's global address book, turning a relatively small stream of requests from attacking machines into a torrent of data sent to the target machines. [HSEC-1.8; Date: 8 March 2012; Source: http://arstechnica.com/business/news/2012/03/how-anonymous-plans-to-use-dns-as-a-weapon.ars]

INFORMATION SYSTEMS BREACHES:

- **Anonymous Leaks Symantec Source Code:** The hacktivist Antisec group has published Symantec Norton AntiVirus 2006 All Platform Source Code on The Pirate Bay. Anonymous, with which Antisec is related, has long boasted of its ownership of Symantec code, and this is its latest release in an ongoing campaign against the security firm. … The latest issuance is dedicated to Jeremy Hammond…who is one the hackers arrested by the authorities this week in relation to Lulzsec attacks on a range of organisations. … Way back when news there had been a leak first broke, the firm confirmed that it was 2006 software that was taken. Though it admitted to only a segment of code being lost, this release seems to contradict that. [HSEC-1.1; Date: 8 March 2012; Source: http://www.theinquirer.net/inquirer/news/2158170/anonymous-leaks-symantec-source-code]
- **Today's #FFF Hack By Anonymous Is A Police Equipment Store:** Anonymous has vowed to do a hack every Friday, calling it the #FFF campaign. Today AntiSec defaced the New York Ironworks, a police equipment supplier that describes itself as 'NYC's finest police equipment & tactical op's gear store.' … While the midweek DDoS on the Vatican is arguably unrelated to recent FBI successes against Anonymous, this is not. The defacement starts "Tribute to Jeremy Hammond, when false heroes fall, true ones rise..." [HSEC-1.10; Date: 9 March 2012; Source: http://www.infosecurity-magazine.com/view/24432/]
- **Adult Site DigitalPlayground.com Hacked: Credit Card Info on 40K Exposed:** The adult Web site DigitalPlayground.com was hacked. A group calling itself TheConsortium has claimed credit for the attack, saying it stole credit card information on 40,000 paying customers and even listened in on a company conference call. The compromise occurred on March 4, according to a message attributed to TheConsortium and posted from the group's Twitter account. The group posted links to an online statement and data dump, allegedly of information stolen from DigitalPlayground's compromised servers. … The attack by TheConsortium followed an almost identical pattern to the earlier LulzSec hacks and the group expressed allegiance to Anonymous and the Antisec movement in its statement. Account credentials for site administrators were posted as were identifying information for around 10,000 Digital Playground customers, including members of the U.S. military. [HSEC-1.10; Date: 9 March 2012; Source: http://threatpost.com/en_us/blogs/adult-site-digitalplaygroundcom-hacked-credit-card-info-40k-exposed-030812]

- **Man Arrested On Suspicion Of Hacking Into Abortion Provider's Website:** A man suspected of hacking into the website of one of the [United Kingdom's] biggest abortion providers is being questioned by police. The 27-year-old, who claims to have links to the hacktivist group Anonymous, was arrested during the early hours of this morning on suspicion of offences under the Computer Misuse Act, Scotland Yard said. It comes after the website of the British Pregnancy Advisory Service (BPAS) was hacked into and defaced on Thursday. Data on the website was also compromised, police said. … Claims later appeared on Twitter that the culprit had accessed the names of women who had undergone terminations and was threatening to release them into the public domain. However, police said the stolen data did not contain any medical details of women who had received treatment. [HSEC-1.10; Date: 9 March 2012; Source: http://www.guardian.co.uk/uk/2012/mar/09/man-arrested-suspicion-hacking-abortion-website]

CYBERTERRORISM & CYBERWARFARE:

- **Chinese Cyber-Warfare A Risk For U.S. Military, Report Says:** Chinese cyber-warfare would pose a genuine risk to the U.S. military in a conflict, for instance over Taiwan or disputes in the South China Sea, according to report for Congress. Operations against computer networks have become fundamental to Beijing's military and national development strategies over the past decade, said the 136-page analysis by Northrop Grumman Corp. It was released on Thursday by the congressionally created U.S.-China Economic and Security Review Commission. The report, based on publicly available information, said Chinese commercial firms, bolstered by foreign partners, are giving the military access to cutting-edge research and technology. [HSEC-1.2; Date: 8 March 2012; Source: http://www.msnbc.msn.com/id/46669768/ns/technology_and_science-security/]

VULNERABILITIES:

- **Google Patches Chrome Bugs Used In Pwnium Contest:** Google has already patched the bugs used by researcher Sergey Glazunov to compromise Chrome on Wednesday as part of the company's Pwnium contest at the CanSecWest conference here. The vulnerability that Glazunov was able to exploit is a universal XSS and bad history navigation bug in the browser. Google on Thursday morning pushed out a new version of Chrome that includes a fix for the vulnerability. [HSEC-1.1; Date: 8 March 2012; Source: http://threatpost.com/en_us/blogs/google-patches-chrome-bugs-used-pwnium-contest-030812]

- **IE 9, On Most Secure Windows Yet, Next Browser To Fall At Hacker Contest:** A fully patched version of Internet Explorer running on the most secure version of Windows yet was the second browser to fall at an annual hacker competition designed to test resistance of internet software to real-world attacks. The attackers were able to take complete control of the underlying laptop by exploiting two previously unknown vulnerabilities in version 9 of the Microsoft browser running on Windows 7 SP 1. Like Tuesday's hacks on Google's Chrome browser, multiple vulnerabilities had be targeted in tandem to penetrate protections developers have added over the past few years, to harden their wares to sophisticated exploits. [HSEC-1.1; Date: 9 March 2012; Source: http://arstechnica.com/business/news/2012/03/ie-9-on-latest-windows-gets-stomped-at-hacker-contest.ars]

- **Apple Unveils iOS 5.1 With Over 80 Security Fixes:** Most of the plugged vulnerabilities involve the WebKit framework used to render web pages in Safari and other applications. Apple warned that visiting a malicious website could lead to a "cross-site scripting attack", an "unexpected application termination", or "arbitrary code execution", according to a security advisory. A number of screen lock bypass issues were fixed, including a race condition issue in the handling of slide to dial gestures. [HSEC-1.1; Date: 8 March 2012; Source: http://www.infosecurity-magazine.com/view/24414/apple-unveils-ios-51-with-over-80-security-fixes/]

GENERAL CYBER/ELECTRONIC CRIME:

- **Facebook: DDoS Attack Didn't Cause European Outage:** Facebook was intermittently unavailable across parts of Europe Wednesday, and at least one national security warning team said that it was due to a distributed denial of service (DDoS) attack. "There is an ongoing DDoS attack towards Facebook. Accessing your Facebook account can temporarily fail," reported Belgium's Computer Emergency Readiness Team (CERT.be) via Twitter Wednesday. … Facebook has blamed the outages on technical faults. … Facebook did not respond to a detailed request for comment about whether the outage had been traced to a DDoS attack, but the evidence has begun to look thin. [HSEC-1.1; Date: 8 March 2012; Source: http://www.informationweek.com/news/security/attacks/232602250]

From: OSINT Branch Mailbox
To: OSINT Branch Mailbox
Subject: DHS-OSE Daily Cyber Report - 2012-03-26
Date: Monday, March 26, 2012 10:06:12 AM
Attachments: DHS_Cyber_Report_2012-03-26.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 26 March 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Cyber Report
26 March 2012

CRITICAL INFRASTRUCTURE PROTECTION:

- **NL Govt Still In Control Of SCADA Systems:** Dutch minister of safety and Justice Ivo Opstelten said the ministry is aware of potential problems with the SCADA (Supervisory Control And Data Acquisition) systems, built to remotely manage and administer machines. Television programme EenVandaag reported that hackers could take over the control of a sewage pump in Veere, to the dismay of Parliament. … Opstelten noted however that while hackers could have taken over the sewage pump in Veere and possibly caused damage, it would not have caused a national disaster. [HSE-1.1; 26 March 2012; Source: http://www.telecompaper.com/news/nl-govt-still-in-control-of-scada-systems]

INFORMATION SYSTEMS BREACHES:

- **Kaiser Permanente Data Breach Affects Thousands Of Employees:** Managed health care consortium Kaiser Permanente has notified thousands of current and former employees that their personal information was found on an external hard drive purchased in a second-hand store in California. Kaiser Permanente said employee names, phone numbers, social security numbers, and other personal information was found on a non-Kaiser external hard drive in a California second-hand store in September…. [HSEC-1.10; Date: 23 March 2012; Source: http://www.infosecurity-magazine.com/view/24739/]

CYBERTERRORISM & CYBERWARFARE:

- **Malicious Code In The IT Supply Chain Threatens Federal Operations:** Agencies that deal with national security data and programs must do more to secure their information technology supply chains, a government watchdog said Friday. Federal agencies aren't required to track "the extent to which their telecommunications networks contain foreign-developed equipment, software or services," the Government Accountability Office report said, and they typically are aware only of the IT vendors nearest to them on the supply chain, not the numerous vendors downstream. That has left IT systems at the Energy, Homeland Security and Justice departments more vulnerable to malicious or counterfeit software installed by other nations' intelligence agencies or by nonstate actors and hackers. [HSEC-1.1; Date: 23 March 2012; Source: http://www.nextgov.com/nextgov/ng_20120323_1655.php]

- **Anonymous Launches Operation Imperva:** Anonymous has declared a new target: Imperva Inc, a security firm…. On 7 March, vatican.va, the official site of the Vatican, suffered a DDoS attack from Anonymous. … Less than a week later, a hacker calling himself Agent_Anon hacked catholica.va via a sql-injection vulnerability. Both of these attacks followed an analysis from security firm Imperva (believed to be an analysis of an earlier attack on the Roman Church) which…says that Anonymous comprises 'a small group of skilled hackers' supported by a larger band of 'laypeople' whose "role is primarily to conduct DDoS attacks by either downloading and using special software or visiting websites designed to flood victims with excessive traffic," and whose skill is from 'very low to modest.' … Anonymous has interpreted Imperva's analysis is damning with faint praise. And it has taken exception. … If this is genuine, it is a new development – this is revenge rather than hacktivism. [HSEC-1.5; Date: 26 March 2012; Source: http://www.infosecurity-magazine.com/view/24752/anonymous-launches-operation-imperva/]

VULNERABILITIES:

- **Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits:** A clever hacker today has to make tough choices . Find a previously unknown method for dismantling the defenses of a device like an iPhone or iPad, for instance, and you can report it to Apple and present it at a security conference to win fame and lucrative consulting gigs. Share it with HP's Zero Day Initiative instead and earn as much as $10,000 for helping the firm shore up its security gear. … But any hacker who happens to know one Bangkok-based security researcher who goes by the handle "the Grugq"–or someone like him–has a third option: arrange a deal through the pseudonymous exploit broker to hand the exploit information over to a government agency, don't ask too many questions, and get paid a quarter of a million dollars–minus the Grugq's 15% commission. [HSEC-1.1; Date: 23 March 2012; Source: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/]

GENERAL CYBER/ELECTRONIC CRIME:

- **Microsoft Leads Seizure Of Zeus-Related Cybercrime Servers:** Microsoft said on Monday it and several partners had disrupted several cybercrime rings that used a notorious piece of malicious software called Zeus to steal US$100 million over the last five years. The company said a consolidated legal case has been filed against those allegedly responsible that for the first time applies the Racketeer Influenced and Corrupt Organizations (RICO) Act. Zeus has been a thorn in the side for financial institutions due to its stealthy nature and advanced spying capabilities that center around stealing online banking and e-commerce credentials for fraud. According to a complaint filed under seal on March 19 in the U.S. District Court for the Eastern District of New York, Microsoft accused the defendants of infecting more than 13 million computers and stealing more than US$100 million over the last five years. The civil complaint lists 39 "John Doe" defendants, many of whom are identified only by online nicknames, such as "Gribodemon" and "Harderman." [HSEC-1.9; Date: 26 March 2012; Source: http://www.computerworld.com/s/article/9225529/]
- **Megaupload Users Targeted With Extortion Scheme:** The recent shutdown of the Megaupload file hosting service by the US authorities is being actively exploited by cyber crooks who are attempting to extort money from the service's users, warns TorrentFreak. The users are being targeted with fake emails ostensibly sent by a German law firm by the name of "Dr. Kroner & Kollegen" that claims to represents Universal, Sony, EMI, Warner and Dreamworks. The emails contain fake IP addresses and timestamps that seemingly prove that the users have downloaded unauthorized copyrighted material from Megaupload, and the "law firm" says that they are liable for fines up to 10,000 Euros. But, it also offers them a way out: pay 147 Euros now, and this all goes away. [HSEC-1.8; Date: 23 March 2012; Source: http://www.net-security.org/secworld.php?id=12644]
- **Call Center Employees Are Selling User Information:** Indian call center employees sell confidential data belonging to users for as little as $0.03, reports the Daily Mail. According to the news outlet, reporters from The Sunday Times have gone undercover in India and have tried to discover if the information that call center employees have access to is in danger of being shared with marketers and crooks. Unfortunately, the answer is yes, as two IT "consultants" were ready to meet and to offer for sale over 45 different sets of information on nearly 500,000 Britons. Among the information contained in the data sets were names, addresses and phone numbers, credit and debit card information … information about loans and mortgages, mobile phone contracts, television subscriptions, medical records and more. Most of the information comes from a number of major banks and financial organizations, and it's usually less than 72 hours old, allowing its buyers to easily take advantage of it. [HSEC-1.1; Date: 23 March 2012; Source: http://www.net-security.org/secworld.php?id=12643]
- **Traders Drop Price Of Silver By Exploiting NASDAQ Vulnerability:** Those in the stock exchange business are highly aware that when it comes to trading every millisecond counts. Experts have long argued that the flaws present in trading systems today can be leveraged to manipulate prices and basically perform fraudulent operations, but a recent incident demonstrated these vulnerabilities. … In simple words, it means that some traders flooded the system which, due to the security holes that exist, caused silver prices to drop considerably. High frequency traders took advantage of the flaws and exploited the NASDAQ silver ETF, Alexander Higgins explains. [HSEC-1.1; Date: 23 March 2012; Source: http://news.softpedia.com/news/Traders-Drop-Price-of-Silver-by-Exploiting-NASDAQ-Vulnerability-260499.shtml]

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Daily Cyber Report - 2012-04-12
Date:	Thursday, April 12, 2012 8:58:18 PM
Attachments:	DHS_Cyber_Report_2012-04-12.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 12 April 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Cyber Report
12 April 2012

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- **Utah's Medicaid Data Breach Worse Than Expected:** A new tally of files stored on a server that contained Medicaid information at the Utah Department of Technology Services (DTS) reveals that 780,000 individuals have been affected by the theft of sensitive information. That's far worse than initial estimates. The data breach occurred on March 30, when a configuration error occurred at the password authentication level, allowing the hacker, located in Eastern Europe, to circumvent DTS's security system. … On Monday DTS, along with the Utah Department of Health (UDOH), announced that an additional 255,000 people had their social security numbers (SSNs) stolen by hackers from a computer server last week. Until last Friday, authorities had estimated that only 25,096 individuals had their SSNs compromised. That brought the revised figure up to 280,096. … Another 500,000 individuals had less sensitive personal information stolen, comprising names, addresses, dates of birth, and medical diagnostic codes, among other information. [HSEC-1.1; Date: 11 April 2012; Source: http://www.informationweek.com/news/healthcare/security-privacy/232900128]

CYBERTERRORISM & CYBERWARFARE:

- **TeaMp0isoN "Phone Bombs" UK Foreign Intelligence Agency MI6:** Members of the hacktivist collective TeaMp0isoN dropped a 24 hour phone bomb, essentially a phone-based denial-of-service attack, on UK's foreign intelligence organization, MI6. The hacktivists compromised a Malaysian server and set it up to execute a script to make calls to the agency's offices for 24 hours straight. "Everytime they picked up the phone the server would play a robot voice which said 'teamp0ison'," explained TriCk, the group's leader. Around 4 hours after the bombing stopped, TriCk prank-called the MI6 offices in London. The audio recording reveals the MI6 representatives who answered the phone becoming upset and threatening to provide law enforcement authorities with the information on TeaMp0isoN. TriCk said that the attack was "because of the recent events where the counter terrorist command and the UK court system has extradited Babar Ahmad, Adel Abdel Bary & a few others to be trialled in the US". [HSEC-1.5; Date: 10 April 2012; Source: http://news.softpedia.com/news/TeaMp0isoN-Phone-Bombs-UK-Foreign-Intelligence-Agency-MI6-264125.shtml]

VULNERABILITIES:

- **Malware-Infected Flash Cards Shipped Out with HP Switches:** Hewlett-Packard sent out a warning to customers after it inadvertently shipped virus-laden compact flash cards with its HP ProCurve 5400zl switches. The flash card wouldn't do anything on the switch itself but "reuse of an infected compact flash card in a personal computer could result in a compromise of that system's integrity," HP warned. It's unclear how the unknown malware got onto the CF cards, which come bundled with 10 Gbps-capable LAN switches, but an infected computer somewhere in the manufacturing process - possible in a factory run by a third-party supplier - is the most likely suspect. [HSEC-1.10; Date: 11 April 2012; Source: http://www.theregister.co.uk/2012/04/11/hp_ships_malware_cards_with_switches_oops]

- **0-Day In Backtrack Linux Found, Patched:** A zero-day vulnerability affecting the last version of Backtrack Linux has been spotted by a student during an Ethical Hacking class organized by the InfoSec Institute. The discovery was made public on InfoSec's own website and detailed by the student himself, who says that the Wireless Interface Connection Daemon (WICD) Backtrack components has several design flaws that can be misused to execute a privilege escalation exploit. … The student and the InfoSec team immediately started on working on a proof-of-concept exploit and the patch for the vulnerability, all of which is provided on the group's site. Backtrack is a Linux distribution popular with penetration testers all over the world because it comes preloaded with hundreds of handy security tools. The vulnerability affects the latest version - Backtrack 5 R2. [HSEC-1.1; Date: 12 April 2012; Source: http://www.net-security.org/secworld.php?id=12740]

GENERAL CYBER/ELECTRONIC CRIME:

- **Symantec Cuts Flashback Infection Estimates In Half:** The high-profile piece of malware that's been estimated to have infected more than 600,000 users of Apple's Mac OS X worldwide, is in considerably fewer machines now, according to a major security firm. In a blog post today, software maker and security firm Symantec said that there are now fewer than half that number of machines with the infection, and that the number of active infections is on a downward trend. "This figure has decreased significantly since then and from our sinkhole data, we have estimated that the number of computers infected with this threat in the last 24 hours is in the region of 270,000, down from 380,000," the company said, adding that it will be monitoring infection levels for the next few weeks. … Apple yesterday announced plans to offer a removal tool for the malware, though it has not offered an estimated time of release. [HSEC-1.8; Date: 11 April 2012; Source: http://news.cnet.com/8301-1009_3-57412598-83/symantec-cuts-flashback-infection-estimates-in-half/]

- **Google Users Targeted With Account Verification Scams:** Scammers have launched a new campaign that's designed to steal Google login usernames and passwords, highly valuable for cybercriminals because they can access a number of services. The emails, which bear the subject "Account Verification", claim that the recipient's recovery email address associated with his or her Google account has changed, and verification is necessary to maintain access to Google accounts. Clicking on the link takes the user to a compromised website which hosts a phishing page, which appears to be a near perfect replica of a Google login page. Once the user provides the account credentials, they are stored in a database controlled by the crooks that run the scam. [HSEC-1.4; Date: 11 April 2012; Source: http://news.softpedia.com/news/Google-Users-Targeted-with-Account-Verification-Scams-264023.shtml]

- **Brothers Who Attacked Nordstrom's eCommerce System Face Jail Time:** Two brothers who used a combination of fraud and business logic attacks against Nordstrom's e-commerce system to defraud the retail giant out of $1.4 million are now facing jail time. Brothers Andrew Chiu, 29, of Anaheim, CA; and Allen Chiu, 37, of Dallas, TX, pleaded guilty on Monday in U.S. District Court in Seattle. The brothers were members of FatWallet.com, an coupon and shopping website that paid cash back rewards for purchases made on several sites, including Nordstrom.com. In January 2010, the brothers found a way to exploit a flaw in Nordstrom's online ordering system by placing orders that would be blocked by Nordstrom with no merchandise being shipped or charges being made. However, Nordstrom unknowingly continued to compensate FatWallet for the order, and the brothers received the cash back credit from FatWallet. [HSEC-1.8; Date: 11 April 2012; Source: http://www.securityweek.com/brothers-who-attacked-nordstroms-ecommerce-system-jail-time]

- **New Anonymous Spinoff Vows To Be Ethical, Quickly Breaks Vow:** Malicious Security, or MalSec, entered the world of hacktivism today with a YouTube manifesto declaring it is veering from the stance of its Anonymous forefathers in favor of a more ethical approach. But at nearly the same time, MalSec posted passwords, email addresses and internal reports stolen from the Development Bank of the Philippines, the Romanian IT firm OanaSoft, the Romanian Minister of European Foreign Affairs and the Romanian Raiffeisen Bank. MalSec also hacked Bhutan's Decentralized Rural Development Project website, apparently in support of Anonymous' recent actions against the Chinese government. MalSec says its exploits will be "a little bit more than for the lulz," and that the group will "tackle critical points" and perform "unified acts of honor" toward a "global revolution." On March 30, MalSec defaced the website of Cayman Islands-based Security Centre Ltd, urging the site's administrators to secure the site and even leaving instructions on how to return it to normal. [HSEC-1.10; Date: 11 April 2012; Source: http://www.securitynewsdaily.com/1719-anonymous-malsec-ethical-hacking.html]

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Daily Cyber Report - 2012-04-13
Date:	Friday, April 13, 2012 10:16:46 AM
Attachments:	DHS_Cyber_Report_2012-04-13.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 13 April 2012 is attached.

(U) Disclaimer: The contents of this unclassified report in no way represent the policies, views, or attitudes of the United States Department of Homeland Security or the United States Government. This report was compiled from various open sources and is intended for appropriate Federal, State, Tribal, and local government agencies and authorities, the private sector, and other entities, that have a need to receive such information for the performance of a lawful governmental or homeland security functions.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Cyber Report
13 April 2012

CRITICAL INFRASTRUCTURE PROTECTION:

- **Tough Love Triumphs: SCADA Vendor Koyo Fixes Basecamp Bugs:** Industrial control system vendor Koyo moved to fix vulnerabilities in its ECOM brand programmable logic controllers (PLCs) after researchers, in January, revealed that the devices were vulnerable to brute force password guessing attacks. The Department of Homeland Security's ICS (Industrial Control System) CERT issued an advisory on Wednesday saying that the company issued a patch for affected ECOM modules that disables a vulnerable Web server and adds a "timeout" feature to prevent brute force attacks on the device password. … Koyo was one of a number of SCADA and ICS vendors whose products were targeted by researchers as part of Project Basecamp, a volunteer effort to expose rampant product insecurity in the ICS sector. [HSEC-1.1; Date: 12 April 2012; Source: http://threatpost.com/en_us/blogs/tough-love-triumphs-scada-vendor-koyo-fixes-basecamp-bugs-041212]

INFORMATION SYSTEMS BREACHES:

- **Icann Confirms System Leak Is To Blame For Top-Level Domain Application Delay:** Internet governing body Icann has confirmed in a statement that a system leak is the reason for its delay of top-level domain (TLD) name applications. The statement made by Icann COO Akram Atallah read, "We have learned of a possible glitch in the TLD application system software that has allowed a limited number of users to view some other users' file names and user names in certain scenarios." Icann apologized for any concerns and explained that it took the system down on Thursday due to an "abundance of caution" after noticing unusual behavior in the system. "We are examining how this issue occurred and considering appropriate steps forward," Icann added. [HSEC-1.1; Date: 13 April 2012; Source: http://www.theinquirer.net/inquirer/news/2167650/icann-confirm-leak-blame-level-domain-application-delay]

CYBERTERRORISM & CYBERWARFARE:

- **West Midland Teens Arrested In Scotland Yard Hotline Hack:** Police have arrested two West Midland teenagers in connection to an ongoing investigation into attacks on the Metropolitan Police counter-terrorism hotline, according to multiple reports. Arrests were based on suspicion of offences underlined in the Malicious Communications Act and the Computer Misuse Act. The names of the arrested have not been released at this time. The news comes after earlier reports of hacking group TeamPoison flooding the Scotland Yard hotline for 24-hours with phone calls. By using a phone based denial-of-service (DOS) attack the hacking collective was able to block all incoming calls to the hotline. Teampoison was able to redirect calls to an outside server which greeted callers with the words "Teampoison." Prior to the arrests, members of the group released recorded phone calls between TeamPoison members and agents of MI6 on Youtube as proof of the prank. [HSEC-1.6; Date: 13 April 2012; Source: http://www.v3.co.uk/v3-uk/news/2167544/west-midland-teens-arrested-scotland-yard-hotline-hack]

- **Operation Defense: Boeing Site Attacked by Anonymous, More to Follow:** The Cyber Intelligence Sharing and Protection Act (CISPA) determined [Anonymous] hacktivists to initiate Operation Defense, an op that has already made a number of victims, including US Telecom, TechAmerica, and more recently, Boeing. … Now, Anonymous has released a new video to reveal the names of other targets. … The list of organizations appointed by Anonymous as being targeted includes AT&T, BSA, COMPTEL, Cyber Space &

Intelligence Association, Exelon, Facebook (again), IBM, Intel, Lockheed Martin, Microsoft, Oracle, Symantec, Verizon Wireless, and many others. According to the hackers, phase two of Operation Defense will commence on May 1 and it will include physical protests at facilities owned by the companies mentioned before. [HSEC-1.6; Date; 13 April 2012; Source: http://news.softpedia.com/news/Operation-Defense-Boeing-Site-Attacked-by-Anonymous-More-to-Follow-264511.shtml]

VULNERABILITIES:

- **Apple Releases Flashback Malware Removal Tool:** Apple Thursday issued a software tool that users can download to remove Flashback, the malware that may have infected between 550,000 and 600,000 Macs at its peak in recent weeks. … Apple says that the update is recommended for "all Mac users with Java installed." Security firm F-Secure on Wednesday also released a free tool to detect and remove Flashback. Meanwhile security software maker Kaspersky Lab said its free "Kaspersky Flashfake Removal Tool" has been "temporarily suspended," and apologized for the inconvenience. [HSEC-1.8; Date: 12 April 2012; Source: http://www.technolog.msnbc.msn.com/technology/technolog/apple-releases-flashback-malware-removal-tool-713704]
- **Oracle To Issue 88 Security Patches On Tuesday:** Oracle is planning to release 88 patches on Tuesday, covering vulnerabilities affecting a wide array of its products, according to a pre-release announcement posted to its website on Thursday. Tuesday's scheduled patch release is larger than Oracle's last quarterly critical patch update in January, when it released 78 fixes. The upcoming patch batch includes six fixes for Oracle's database, three of which can be exploited remotely without a username and password. … Another 11 patches cover Oracle Fusion Middleware, with nine being remotely exploitable without authentication. [HSEC-1.1; Date: 12 April 2012; Source: http://www.computerworld.com/s/article/9226169/]
- **Facebook SDK Hole Leaves Accounts Vulnerable:** Developer David Poll discovered that a vulnerability in the Facebook SDK for Android grants specially crafted Android apps unauthorized access to the smartphone owner's Facebook account. Apps such as foursquare use the SDK as a convenient way of reading users' Facebook profiles or posting photos to their walls; usually, this requires additional permissions to be requested from the user. Once those permissions are granted, the app receives an access token from the Facebook server that, until revoked, enables it to perform the requested actions. Poll found that, with the required permissions in place, the Facebook SDK writes a URL that contains the token to a log file on the smartphone – and this log file is accessible by any app that has been given permission to "Read Sensitive Log Data" during installation. [HSEC-1.1; Date: 12 April 2012; Source: http://www.h-online.com/security/news/item/Facebook-SDK-hole-leaves-accounts-vulnerable-1519859.html]
- **Security Vulnerability In NVIDIA's Proprietary Linux Drivers Fixed:** A new version of NVIDIA's proprietary UNIX graphics drivers for Linux, Solaris and FreeBSD fixes a security vulnerability (CVE-2012-0946) that allowed attackers to read and write arbitrary system memory in order to, for example, obtain root privileges. To take advantage of the vulnerability, an attacker must have access permission for some device files – which, for systems with these drivers, is typically the case for users who can launch a graphical interface as 3D acceleration and some other features cannot be used otherwise. [HSE-1.1; Date: 12 April 2012; Source: http://www.h-online.com/security/news/item/Security-vulnerability-in-NVIDIA-s-proprietary-Linux-drivers-fixed-1520095.html]

GENERAL CYBER/ELECTRONIC CRIME:

- **Controversy Erupts Over Microsoft's Recent Takedown Of A Zeus Botnet:** Microsoft's unprecedented aggressive legal strategy in botnet takedowns came under fire from researchers in the Netherlands, charging that the software giant's most recent botnet dismantlement operation has ultimately damaged international law enforcement and private research investigations. Michael Sandee, principal security expert at Netherlands-based Fox-IT, wrote in a blog post today that rather than truly injuring the Zeus botnet operations last month, Microsoft instead has hampered investigations into these operations by its actions last month of removing and confiscating two of the command-and-control (C&C) servers under a federal court order. … Richard Boscovich, senior attorney for Microsoft's Digital Crimes Unit, said in a statement that Fox-IT's post "is based at least in part on some factual misunderstandings about the operation which we are more than happy to discuss with Fox IT." [HSEC-1.9; Date: 12 April 2012; Source: http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232900239/]

From: OSINT Branch Mailbox
To: OSINT Branch Mailbox
Subject: DHS-OSE Daily Cyber Report - 2012-04-23
Date: Monday, April 23, 2012 9:59:28 AM
Attachments: DHS_Cyber_Report_2012-04-23.pdf

Classification: UNCLASSIFIED

(U) The DHS Daily Cyber Report for 23 April 2012 is attached.

(U) Disclaimer: The contents of this unclassified report in no way represent the policies, views, or attitudes of the United States Department of Homeland Security or the United States Government. This report was compiled from various open sources and is intended for appropriate Federal, State, Tribal, and local government agencies and authorities, the private sector, and other entities, that have a need to receive such information for the performance of a lawful governmental or homeland security functions.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) These materials, including copyrighted materials, are intended for 'fair use' as permitted under Title 17, Section 107 of the United States Code ('The Copyright Law'). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security
E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Cyber Report
23 April 2012

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- Nothing significant to report

CYBERTERRORISM & CYBERWARFARE:

- **Hackers Targeting Governments With Hijacked Sites:** Malicious code planted within compromised pages has become the latest method for attackers targeting government organizations, according to research from security firm Zscaler. The firm reported a number of government-affiliated sites that have been found to contain code that directs users to attack servers. The most recent site to become infected was that of the French Budget Minister. … The attack is the latest in what Zscaler sees as a string of site hijackings aimed at government-controlled domains. … Zscaler chief executive…believes the attacks are not the work of profit-minded criminals looking to harvest bank details, but rather state-sponsored operations aimed at infecting government workers and other high-value targets. [HSEC-1.8; Date: 21 April 2012; Source: http://www.v3.co.uk/v3-uk/news/2169452/hackers-targeting-governments-hijacked-sites]

- **US Website Covering China's Bo Xilai Scandal Hacked:** A US-based Chinese-language website that has reported extensively on the Bo Xilai scandal in China says it was crippled for several hours by a concerted hacking attack. The Boxun website had to move to a new webhost after the denial-of-service attack on Friday…. Boxun's original webhost, Name.com, told the Associated Press news agency that the hack was one of the biggest in the company's history. It reportedly followed an emailed threat that it would be attacked if it did not disable the site. It is not clear who launched the attacks, but the manager of Boxun.com…was quoted as saying he believed they were ordered by China's security services. [HSEC-1.2; Date: 21 April 2012; Source: http://www.bbc.co.uk/news/world-asia-china-17796810]

VULNERABILITIES:

- **New Version Of OpenSSL Closes Security Holes In ASN1 Parser:** Tavis Ormandy from the Google Security Team has notified the OpenSSL developers of a security hole in the current version of their open source library. ... According to the official OpenSSL advisory and Ormandy's message, the issue affects applications that process external X.509 certificates or public RSA keys. However, the remaining information about the applications that are affected, and the potential consequences, is rather cryptic. [HSEC-1.1; Date: 20 April 2012; Source: http://www.h-online.com/OpenSSL-closes-security-holes-in-ASN1-parser.html]

- **Icann Security Chief Rules Out Malicious Attack Behind gTLD Submission Glitch:** The Internet Corporation for Assigned Names and Numbers (Icann) has revealed more details on the problems afflicting its submission system for generic top level domains that forced it to take the system offline…. The organisation first announced there was an issue earlier this month, revealing that some information submitted by firms applying for a new domain may have been visible to one another in the process. [T]he organisation's chief security officer…said that having studied the issue, he was confident there was no malicious intent behind the glitch. [HSEC-1.1; Date: 20 April 2012; Source: http://www.v3.co.uk/icann-security-chief-rules-attack-glitch]

- **100 Million Users Might Be Affected By A Social Network Vulnerability:** Do it yourself social networking company Ning is reportedly suffering from a slight security problem that could affect 100 million users. Ning lets people set up their own gasbag social networking channels and is used by people like the pop group Radiohead. According to a Dutch report a problem with its security could leave them wide open to account hijackers. A Dutch web site called Web Wereld says that two students, Angelo Geels and Alex Brouwer have exploited cookies to gain login control over Ning user accounts. They used a proof of concept that showed they could access 90,000 accounts and 100 million users, but had no intention of exploiting it for malicious purposes. [HSEC-1.1; Date: 20 April 2012; Source: http://www.theinquirer.net/inquirer/news/2169403/100-million-users-affected-social-network-vulnerability]
- **TV-Based Botnets? DoS Attacks On Your Fridge? More Plausible Than You Think:** It's still premature to say you need firewall or antivirus protection for your television set, but a duo of recently diagnosed firmware vulnerabilities in widely used TV models made by two leading manufacturers suggests the notion isn't as far-fetched as many may think. The most recent bug, found in a wide range of high-definition TVs from Samsung, was disclosed on Thursday by Luigi Auriemma, an Italy-based researcher who regularly finds security flaws in Microsoft Windows, video games, and even the industrial-strength systems used to control dams, gas refineries, and other critical infrastructure. … His discovery came two weeks after a separate researcher reported a DoS vulnerability in Sony Bravia TVs. [HSEC-1.1; Date: 22 April 2012; Source: http://arstechnica.com/business/news/2012/04/tv-based-botnets-ddos-attacks-on-your-fridge-more-plausible-than-you-think.ars]

GENERAL CYBER/ELECTRONIC CRIME:

- **Flashback Botnet Not Shrinking, Huge Numbers Of Macs Still Infected:** Contrary to reports by several security companies, the Flashback botnet is not shrinking, the Russian antivirus firm that first reported the massive infection three weeks ago claimed today. Dr. Web, which earlier this month was the first to report the largest-ever successful malware attack against Apple's OS X, said Friday that the pool of Flashback-infected Macs still hovers around the 650,000 mark, and that infections are continuing. Also on Friday, Liam O Murchu, manager of operations at Symantec's security response center, confirmed that Dr. Web's numbers were correct. … According to Dr. Web, counts by others were incorrect because of how the malware calculates the locations of command-and-control (C&C) servers, and how it communicates, or tries to, with those domains. [HSEC-1.8; Date: 20 April 2012; Source: http://www.computerworld.com/s/article/9226429/]
- **Anonymous Targets Formula 1 With DDoS Attacks In #OpBahrain:** In its latest operation dubbed "#OpBahrain", Anonymous supporters launched a series of DDoS attacks against web sites connected to the wildly popular Formula 1 Racing series. Included in the attacks were domains associated with the official F1 Web site, Formula1.com along with f1.com, both of which resolve to the IP address 195.219.144.30. The moves are in protest to the upcoming Bahrain Grand Prix scheduled to take place this weekend in Bahrain. According to Anonymous, the government of Bahrain "continues to use brutal and violent tactics to oppress the popular calls for reformation." [HSEC-1.10; Date: 20 April 2012; Source: http://www.securityweek.com/anonymous-targets-formula-1-ddos-attacks-opbahrain]
- **Thousands Of Attempts To Hack Abortion Provider BPAS:** Thousands of attempts have been made to hack into the computers of Britain's largest provider of abortion services, BPAS, the BBC has learned. Last month, a man was jailed for stealing the details of 10,000 women who had sought advice from BPAS. In the five weeks since his arrest, 2,500 other attempts have been made to hack into BPAS's systems. BPAS said all these hacking attempts had been foiled. … BBC correspondent Michael Buchanan said that research into the IP addresses of the computers used during the attempted hacking had revealed that almost half came from the United States. But he said that the nature of hacking meant it was not possible to say the hackers were based in the US. [HSEC-1.10; Date: 20 April 2012; Source: http://www.bbc.co.uk/news/uk-17765904]

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Homeland Security Central Digest - 2012-01-05
Date:	Thursday, January 05, 2012 7:38:23 AM
Attachments:	DHS Daily Digest - 20120105.pdf

Classification: UNCLASSIFIED

(U) The DHS Homeland Security Central Digest for 05 January 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) Articles and resource documents come from open source information and are posted to the Homeland Security Central website on Intelink-U. For information on establishing an Intelink-U account, please visit http://ra.intelink.gov.

(U) The Homeland Security Central Digest contains full article text and may contain copyrighted material whose use has not been specifically authorized by the copyright owner. This information is available to DHS, in the interest of illuminating incidents and events that may have an impact on national security and critical infrastructure protection. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at:
(b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security

E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Digest
5 January 2012

Reinsurer: Record Natural Disaster Losses In 2011

The devastating earthquakes in Japan and New Zealand made 2011 the costliest year yet for the insurance industry in terms of natural disaster losses, a leading reinsurance company said Wednesday. The total economic cost last year from natural disasters — including uninsured losses — totaled about $380 billion. [HSEC-2.2]

New Mexico Scientist Was Building Bombs At Home Before Death, Sheriff Says

A New Mexico sheriff said a retired Sandia Labs scientist was apparently building bombs at his home before he died. [HSEC-10.1]

Flash Of An iPad Gets Man Past Border Security

A Canadian man who left his passport at home discovered an unusual way to get through U.S. Customs – with the help of his iPad. Martin Reisch says a border officer let him cross into the United States from Quebec after he presented a scanned copy of his passport on the computer tablet and his driver's licence. [HSEC-1.7]

Top TSA Checkpoint Finds In 2011 Include Over 1,000 Guns, C4

The Transportation Security Administration has found 1,200 guns, snakes, C4 explosives and inert landmines in the past year at airport checkpoints around the country. [HSEC-8.1]

Cyber Attacks Expected To Rise In 2012

A late December story about hackers taking down Stratfor Global Intelligence's website and stealing credit card numbers to use to donate money to nonprofits was a reminder that everyone -- governments, businesses, think tanks and individuals -- must continue to strengthen their vigilance and online security in 2012. [HSEC-1.1]

Why Qatar, World's Richest Nation, Is Hosting Taliban Talks

Qatar, as diplomats say, likes to "punch above its weight." This arid peninsula in the Persian Gulf is smaller than Connecticut but played a leading role in helping Libyan rebels oust Moammar Gadhafi and has been at the heart of Arab League sanctions against Syria. It's now facilitating talks on the Afghan conflict by allowing the Taliban to open a liaison office in its capital, Doha. [HSEC-8.8]

12 Year Sentence For Smuggling 5,000 Kilos Of Marijuana

U.S. District Judge Nelva Gonzales Ramos sentenced an Alamo, Texas man to 145 months in prison for smuggling more than 5,000 kilos of marijuana. [HSEC-5.10]

Massive Grass Fire Burns In Eastern Texas

The U.S. Fish and Wildlife Service is battling a large grass fire in the marshlands of Jefferson County, Texas, an agency official told CNN on Tuesday. [HSEC-2.2]

Lake Wildwood Couple Plead Guilty To Federal Drug Charges [CA]
A Lake Wildwood husband and wife have pleaded guilty to federal charges for their role in an international drug-smuggling ring. [HSEC-5.10]

Suspected Smuggling Boat Found Abandoned Off Santa Barbara Coast
The Santa Barbara County Sheriff's Department is asking the public to be on the lookout for Mexican smuggling boats that have been spotted recently off the Santa Barbara coastline, according to a statement issued by the agency Tuesday. [HSEC-3.3]

Florida Growers Brace For Cold Snap
Florida grower-shippers are preparing for the season's first night of subfreezing temperatures. Temperatures are forecast to fall as low as 23 degrees during the early morning hours of Jan. 4 in the Plant City, Fla., growing region, the hub for U.S. winter strawberries. [HSEC-2.2]

Full Text of all new articles....

Reinsurer: Record Natural Disaster Losses In 2011

By Geir Moulson
The Associated Press
January 4, 2012

The devastating earthquakes in Japan and New Zealand made 2011 the costliest year yet for the insurance industry in terms of natural disaster losses, a leading reinsurance company said Wednesday.

Munich Re AG said in an annual report that insured losses last year totaled $105 billion — exceeding the previous record of $101 billion set in 2005, when losses were swollen by claims from Hurricane Katrina in New Orleans.

The company said the total economic cost last year from natural disasters — including uninsured losses — totaled about $380 billion. That was far above the 2005 record of $220 billion.

Japan's earthquake and tsunami in March caused overall losses of $210 billion and insured losses of between $35 billion and $40 billion, Munich Re said. That didn't include the consequences of the subsequent meltdowns at the Fukushima Dai-ichi nuclear plant, which resulted in the evacuation of a wide swath of land.

The second most costly disaster for insurers, at $13 billion, was the February quake that devastated much of the New Zealand city of Christchurch. Overall losses came to $16 billion.

Munich Re noted that last year's sequence of natural disasters was very rare, and that 2011 brought catastrophes expected only once every 1,000 years or more. Normally, weather-related events are the chief cause of losses, it said.

"Even if it seems hard to believe given recent events, the probability of earthquakes has not increased," said Peter Hoeppe, the head of Munich Re's risk research unit.

He added, however, that "these severe earthquakes are timely reminders that the decisions on where to build towns need careful and serious consideration of these risks, especially where certain buildings are concerned, above all nuclear power plants."

Building codes in earthquake-prone regions need to be made even stricter, he argued.

Last year's third-costliest disaster for insurers was Thailand's worst flooding in half a century, which began in late July and continued for months.

Insured losses came to $10 billion, while total overall losses were estimated at $40 billion, making it Thailand's costliest-ever natural disaster, Munich Re said.

Severe storms and tornadoes in the United States in late April cost insurers $7.3 billion and led to overall damage worth $15 billion. Hurricane Irene, which hit the Caribbean and U.S. in late August, caused insured losses of $7 billion and total losses of $15 billion.

Still, Munich Re said losses from North Atlantic hurricanes were "moderate" in 2011, with only three major named storms making landfall in the United States.

Reinsurers offer backup policies to companies writing primary insurance policies. Reinsurance helps spread risk so that the system can handle large losses from natural disasters.

Munich Re has measured natural disaster costs since 1980.

[Return to top] *Topic Area: Disasters*

New Mexico Scientist Was Building Bombs At Home Before Death, Sheriff Says

FOX News/Associated Press
January 4, 2012

A New Mexico sheriff said a retired Sandia Labs scientist was apparently building bombs at his home before he died.

Torrance County Sheriff Heath White tells KOB-TV it appears 81-year-old David O'Keefe spent his retirement on the outskirts of Estancia continuing his work up until he died a few months ago.

White says O'Keefe was trying to make a new type of explosive and was experimenting with different chemicals and different compounds to make that explosive, which put neighbors within a half mile in great danger.

Deputies discovered the explosives Saturday when the property owner went to check on the home and found the chemicals.

White says cleanup will take some time.

[Return to top] *Topic Area: Explosive Devices*

Flash Of An iPad Gets Man Past Border Security

By Andy Blatchford
The Canadian Press
January 3, 2012

A Canadian man who left his passport at home discovered an unusual way to get through U.S. Customs – with the help of his iPad.

Martin Reisch says a border officer let him cross into the United States from Quebec after he presented a scanned copy of his passport on the computer tablet and his driver's licence.

Mr. Reisch's entrance into the U.S. without a mandatory, hard copy travel document hints how, in some cases, stricter rules at the thickened American border may still have some flexibility in practice.

He said he was about a half-an-hour drive from the Vermont border last week when he realized he had forgotten his passport.

Mr. Reisch quickly remembered that a scanned copy of the document was stored on his iPad, and instead of turning his car around for the two-hour drive home, he decided to give it a shot.

"I figured I'd try, and in the worst case, I would have to go home," he said Tuesday.

Mr. Reisch, 33, said he explained his situation to the customs officer, who seemed mildly annoyed when he handed him the iPad.

"He kind of gave me a stare, like neither impressed nor amused," he said of their exchange last Friday in southern Quebec.

The agent took the iPad and the driver's licence into the border office for about five minutes before coming back outside to give Mr. Reisch the green light. The officer also wished him happy holidays.

"He was very nice about it," Mr. Reisch said.

"I think a good part of it had to do with the fact that it was the holidays and I seem like a nice-enough person."

U.S. Customs and Border Protection says it will accept documentation such as a passport, an enhanced driver's licence or a Nexus pass from Canadian citizens entering at land crossings. The list doesn't mention facsimiles, such as scans and photocopies.

A spokeswoman for the department did not immediately respond to questions Tuesday on whether scanned passports are also commonly accepted at U.S. points of entry.

Two people who follow border issues carefully called the case intriguing, but they had different interpretations of what it might mean for Canadian travelers.

Professor Heather Nicol, a border-security expert from Trent University, said Mr. Reisch's experience is likely one of many unspoken exceptions carried out at U.S. border crossings.

"There is some wiggle room," said Prof. Nicol, a political geographer at the Peterborough, Ont., university.

"What it suggests is that this whole standardization process is a little bit of a shell game because we're told it's not about individuals, it's about data sets. But sometimes the experience is very individual."

Prof. Nicol said a customs officer may consider factors such as the credentials of the traveler and how frequently they enter the U.S.

She added that the personality and job experience of the officer as well as the traffic volume at the point of entry may also play roles.

"It's unusual, but I don't think it's unheard of," said Prof. Nicol, who hadn't heard of any cases like this one before.

But another observer argued that Mr. Reisch's crossing without a mandatory travel document is likely an isolated case. Canadians have had to present more than just a regular driver's licence at U.S. Customs for a couple of years.

New Democrat MP Brian Masse, who represents the Ontario border city of Windsor, said he's been working on customs issues for more than a decade and has never heard of anything like it.

Mr. Masse noted it's interesting that Mr. Reisch had such an easy time crossing while many Canadians still face border hassles under systems like the Nexus program, a special pass designed to speed up the process for its users.

"It runs counter to everything else that we've seen," Masse said.

"I think this guy just got lucky."

He said it also raises troubling security questions because information and photos on scanned passports can easily be altered.

"Basically, any kid in grade school can pretty well do something with it," said Mr. Masse, who is open to digital passports as long as their security is assured.

Mr. Reisch, who went to Vermont for the day to see friends and snap landscape photos, said he also showed the passport on his iPad to Canadian Customs on the way home although it wasn't necessary.

The Canada Border Services Agency says a passport is only one of several documents accepted at customs for returning Canadian citizens and permanent residents. The border officers will also accept alternatives like a Canadian birth certificate and a citizenship card.

When asked Tuesday about Mr. Reisch's case, a spokeswoman for the Canadian border agency declined to comment and suggested the question be directed to U.S. Customs.

Mr. Reisch, who said he travels to the U.S. about a dozen times a year, hopes border officials eventually make digital identification an official form of travel document.

"I like the idea of things being catalysts for change," said the freelance photographer and videographer, who noted that many airlines now accept digital boarding passes stored on smartphones.

"It's a recognized form of checking in (on airlines), so I see the future as 100 per cent being able to cross with your identity on a digital device – it's just a matter of time."

[Return to top] *Topic Area: Border Security*

Top TSA Checkpoint Finds In 2011 Include Over 1,000 Guns, C4

By Mark Rockwel
Government Security News
January 4, 2012

The Transportation Security Administration has found 1,200 guns, snakes, C4 explosives and inert landmines in the past year at airport checkpoints around the country.

The agency listed its "Top Ten" finds of the year on its web site on Jan. 2. The most significant discoveries, it said, not only included dangerous items like edged weapons, loaded guns and explosives, but offbeat things like science experiments that look like bombs and live animals.

"Some are dangerous, some simply look dangerous and can cause major delays, and others are just plain weird," said the post.

The site termed the discovery of small chunks of C4 military explosives found in the bags of a U.S. Army Private at Yuma International Airport in Arizona last July as the number one find of the year by its security agents. The half ounce of explosive was found in the checked bag of a 19-year-old soldier, concealed in a tobacco can. TSA said its agents made the discovery in the checked bag using an Explosive Trace Detection (ETD) test. The private, Christopher Wey, was subsequently charged with attempting to carry an explosive on an aircraft and transportation of a stolen explosive. TSA said he was apparently bringing the material home to show his parents and officials had said he had no apparent intent to harm anyone.

Although it didn't make the top ten list as the discovery happened on the last day of 2011, TSA agents made a similar find at a Texas airport. On New Year's Eve, TSA agents detected explosives in the bags of another travelling soldier. The FBI arrested Trey Atwater, of Hope Mills, NC, on Dec. 31, while he was going through security at Midland Airport in Texas. The FBI said they arrested Atwater on charges of attempting to carry concealed explosives onto an aircraft. Atwater has claimed he used the explosives as a demolition expert while serving in Afghanistan, but didn't know they were still in his bag. Atwater had also been detained days earlier at the Fayetteville, N.C., airport after security agents found a military smoke grenade in his carry-on bag.

The second top find on the agency's list included the discovery of a loaded .380 pistol strapped to the ankle of a passenger passing through a check point in Detroit Metro Airport on Dec. 13. The 76-year-old passenger, said the agency, forgot the pistol was there.

The third top find was the total number of guns found during the year at checkpoints across the country. The

agency said it found over 1,200 firearms, some loaded or with rounds in their chambers. For the most part, TSA accounted for the discoveries as passengers' forgetting their presence in luggage.

The agency also noted that it found knives concealed in a book in a passenger's bag at Washington National, as well as inert landmines in bags at Salt Lake City airport, a stun gun disguised as a smart phone in Los Angeles, a flare gun and seven live flares in Norfolk, as well as assorted live snakes, turtles, birds and fish concealed in luggage at Miami and Los Angeles.

TSA's top finds

[Return to top] *Topic Area: Airports & Airlines*

Cyber Attacks Expected To Rise In 2012

Longmont Times-Call
January 4, 2012

A late December story about hackers taking down Stratfor Global Intelligence's website and stealing credit card numbers to use to donate money to nonprofits was a reminder that everyone -- governments, businesses, think tanks and individuals -- must continue to strengthen their vigilance and online security in 2012.

Though the group Anonymous originally was reported as the perpetrator of the Stratfor attack, an Anonymous member issued a press release the day after the attack denying responsibility.

Whoever was responsible, one thing is undisputed: Such "hacktivism" is expected to increase this year, along with every other form of cyber attack, whether it's the pilfering of personal information for identity theft and financial fraud or one government's theft of another's secrets or the emails we all get that want us to open a document or click on a link, thus opening our computers up to attack.

We have to trust that our federal, state and local governments are protecting their online information with the best methods available. We have to trust that the company we just gave our credit card or bank account information to for an online purchase won't let that information get stolen. We have to trust ourselves not to open that attachment from someone we don't know or fall for the numerous other email scams.

But as the Stratfor attack illustrates, along with all the other well-publicized cyber attacks last year, as long as personal information and other sensitive information are floating around in cyber space, someone out there is likely trying to uncover it and use it for malicious purposes.

There's much folks can do to protect themselves on their personal computers. It appears many companies still need to improve their online security.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Why Qatar, World's Richest Nation, Is Hosting Taliban Talks

By Tim Lister
CNN
January 4, 2012

Qatar, as diplomats say, likes to "punch above its weight." This arid peninsula in the Persian Gulf is smaller than Connecticut but played a leading role in helping Libyan rebels oust Moammar Gadhafi and has been at the heart of Arab League sanctions against Syria. It's now facilitating talks on the Afghan conflict by allowing the Taliban to open a liaison office in its capital, Doha.

Qatar is also home to the pan-Arab news channel Al Jazeera, a thorn in the side of many Arab regimes past and present. It is a major player in the energy industry, with vast reserves of natural gas, and -- perhaps in an effort to outflank Dubai as the playground of the Gulf -- is due to host the soccer World Cup in 2022.

It helps that the emirate is fabulously wealthy, with the highest per-capita gross domestic product in the world. It can fund ambitious initiatives -- to help fund the Palestinian Authority, for example, or provide cash and weapons to the Libyan rebels. Now it's exploiting long-held ties with the Taliban to provide a platform between the group and the international community, and especially the United States.

As far back as 2001, before the group was ousted in Afghanistan, the Qataris hosted Taliban delegations. And in the past year, thanks to its hyperactive diplomacy under Prime Minister (and Foreign Minister) Hamid bin Jassim Al-Thani, the emirate has emerged as a regional power broker -- to the consternation of its larger neighbor, Saudi Arabia.

Qatar's growing dynamism within the Arab League has been most evident amid the unrest in Libya and Syria. It was one of two Arab states to play a role in enforcing the no-fly zone over Libya. And according to journalists in western Libya last spring, Qatari advisers were working with Libyan rebels in the Nafusa Mountains as well as supplying anti-tank missiles and other weaponry to rebel forces in the east.

In November, Qatar forged a package of sanctions against the regime of Bashar al-Assad that was adopted by the Arab League, provoking an attack on its embassy in Damascus and the withdrawal of the Qatari ambassador. It lobbied other Arab states hard, telling them that effective Arab action was required to avoid "foreign interference" in Syria. Qatar was also ready to use the power of the purse with Syria by canceling projects there.

As part of intensive efforts to build a relationship with the United States, Qatar has allowed U.S. forces to use the al-Udeid air base for operations in Iraq, Afghanistan and Somalia. It also hosts the forward headquarters of the U.S. Central Command.

Over the past 10 years, Qatar has also offered to be the go-between in Iran for successive U.S. administrations. According to a 2006 U.S. diplomatic cable, Foreign Minister Al-Thani told a U.S. official, with some pride: "Qatar talks to Iran as an equal, and this is important."

The two countries are joined at the hip, as they share vast natural gas reserves under the Gulf. And it is a principle of Qatari diplomacy that it will cultivate groups that won't talk to each other -- Hamas and Iran as well as Washington. Qatar also offered to help the United States improve relations with Sunni tribal leaders in Iraq at the height of the insurgency there.

The emir, Hamad Bin Khalifa Al-Thani, and his family drive Qatari policy and have proved themselves agile negotiators with a grasp of the intricacies of Middle East politics. U.S. diplomatic cables describe Qatari officials as well-prepared with a detailed understanding of the nuances of their complex neighborhood.

The Arab Spring has worked in Qatar's favor. One of the few states where no protests have occurred, it has taken advantage of Saudi caution and upheavals in Egypt and Syria to carve out an assertive regional role.

But Qatar's activism generates plenty of resentment. The populism of Al Jazeera has infuriated Arab regimes. The emir fends off complaints about Al Jazeera's reporting, telling CNN's Wolf Blitzer last year: "Of course it's not necessary I will agree with what Al Jazeera say. Actually, Jazeera caused for me a lot of problems."

Similarly, the Saudis are suspicious of Qatar's open channel with Iran. President Ali Abdullah Saleh of Yemen put an end to Qatari efforts to mediate between his government and Huthi rebels. And President Hamid Karzai recalled the Afghan envoy in Doha in December because he'd been kept in the dark about contacts with the Taliban.

But the Al-Thanis are not afraid to ruffle feathers. In the diplomatic world, as one Gulf commentator observed,

Qatar is proof that size isn't everything.

[Return to top] *Topic Area: Counter Terrorism*

---

12 Year Sentence For Smuggling 5,000 Kilos Of Marijuana

KRISTV.com
January 3, 2012

U.S. District Judge Nelva Gonzales Ramos sentenced an Alamo, Texas man to 145 months in prison for smuggling more than 5,000 kilos of marijuana.

44-year-old Hector Garza Martinez was arrested at the Falfurrias checkpoint in July during a secondary inspection of his tractor-trailer.

Prosecutors say a K-9 unit alerted authorities to 470 cellophane wrapped bundles of marijuana hidden in a load of cotton seed.

Martinez plead guilty in October.

The seizure was the largest at the Falfurrias checkpoint for 2011.

The bust occurred on the busy July 4th weekend.

[Return to top] *Topic Area: Illegal Drug Trafficking*

Massive Grass Fire Burns In Eastern Texas

By Nick Valencia
CNN
January 3, 2012

The U.S. Fish and Wildlife Service is battling a large grass fire in the marshlands of Jefferson County, Texas, an agency official told CNN on Tuesday.

The fire began Monday afternoon about 12 miles west of Sabine Pass and about 200 yards from the Intracoastal Waterway, Jim Stockie, spokesman for the fish and wildlife service said. He estimated the area burned by Tuesday afternoon to be between 10,000 and 12,000 acres, but he said the fire was not threatening any structures.

Smoke from the blaze was drifting into the Houston/Galveston area more than 100 miles from the fire.

Just a dozen firefighters were working the blaze, Stockie said.

"We don't like to put firefighters out in a sea of grass. We retreat to levies and burn off the fuel," Stockie said.

Texas has suffered its worst fire season in state history with more than 3.5 million acres burned, according to state officials.

In October, the Bastrop Complex Fire torched more than 1,500 homes and 34,000 acres of land north of Austin before officials were able to contain it, the Texas Fire Service said.

An unusual La Nina weather pattern led to a nearly 11-month fire season in the state, fire service spokeswoman April Saginor said.

A survey released last month by the Texas Forest Service estimated between 100 million and 500 million trees, or 2% to 10% of the state's 4.9 billion trees, were killed by the severe drought and consequent fires. The dry spell that began in 2010 was the worst the state has seen since 1895, Texas Lt. Gov. David Dewhurst has said.

The drought conditions also caused concern for the state's water supply, especially in smaller towns.

[Return to top] *Topic Area: Fire & Wildfire*

Lake Wildwood Couple Plead Guilty To Federal Drug Charges [CA]

By Liz Kellar
TheUnion.com
January 4, 2012

A Lake Wildwood husband and wife have pleaded guilty to federal charges for their role in an international drug-smuggling ring.

Michael and Pamela Murphy were arrested in late April 2011 by agents from the U.S. Drug Enforcement Agency and the U.S. Department of Homeland Security Investigations. They later were released on bail.

The Murphys had moved into a house in the 13000 block of Lake Wildwood Drive the previous fall, neighbors said.

According to the complaint filed in federal court in Seattle, the couple was part of a drug trafficking organization that also smuggled cocaine from Mexico into California. Twenty other people were arrested in the case, according to the complaint.

At least seven other people have pleaded guilty to related charges.

The organization was smuggling 1,000 to 2,000 pounds of marijuana a month from Canada to Chicago, Detroit, St. Louis, Atlanta and Los Angeles. Members then used the proceeds to buy cocaine in Mexico — about 100 to 200 kilos a month — and smuggle it through the United States into Canada, according to the complaint.

The Canadian marijuana was being supplied by Hell's Angels in British Columbia, and the ring as a whole was prepared to use violence, according to court documents.

Federal agents searched the Murphys' home and allegedly found about $316,000 in cash, some of which was bundled in plain view on the kitchen counter. They also allegedly found money-counting machines.

Pamela Murphy claimed she kept the cash for her personal use, because she does not use banks. She told agents she and her husband were in the antiques business, and that her husband also did engineering and design work, according to the complaint.

Michael Murphy — known as "Old Guy," "OG" or "Steve" — pleaded guilty to conspiracy to distribute controlled substances, and conspiracy to commit money laundering; his plea was accepted in federal court on Dec. 29.

He faces at least 10 years and a possible maximum life sentence for the first charge, and as many as 20 years for the second count. It was not clear when sentencing would be scheduled.

Michael Murphy admitted using aircraft that he owned to transport marijuana, and to recruiting other pilots. He flew marijuana to locations across the United States, and he admitted to distributing more than 1,000 kilograms as part of the conspiracy.

He would also pick up cash from customers or other members of the drug ring, and deliver it back to California.

Pamela Murphy — code name "Betty" — pleaded guilty to one count of conspiracy to commit money laundering. She faces as much as 20 years in prison, but the plea agreement calls for two years.

She admitted that her husband and others would deliver narcotics proceeds to her. After she counted the cash, her husband would take it to a "banker" in Los Angeles, according to court documents.

Pamela Murphy also admitted to being paid $7,000 a month to count the drug proceeds, and she added she was responsible for between $1 million and $2.5 million in laundered cash.

Suspected Smuggling Boat Found Abandoned Off Santa Barbara Coast

By Lara Cooper
Noozhawk.com
January 3, 2012

The Santa Barbara County Sheriff's Department is asking the public to be on the lookout for Mexican smuggling boats that have been spotted recently off the Santa Barbara coastline, according to a statement issued by the agency Tuesday.

Early Monday morning, an empty boat was discovered abandoned off the coast north of Refugio Beach by off-duty sheriff's deputies commuting to work. Responding personnel confirmed that the vessel was a Panga boat, a small open watercraft with several outboard motors.

"They are commonly used by fishermen in developing countries and have become increasingly popular with smugglers who are transporting illegal immigrants, narcotics or other contraband from Mexico to the United States," the Sheriff's Department said in the statement. "Although the boat was empty, there was evidence it was used for illicit drug trafficking."

Panga boats have made illegal runs from Mexico to as far north as the San Francisco Bay Area. They are typically 19 to 28 feet in length, but the boat discovered Monday was 30 feet long and capable of transporting up to 2,000 pounds of cargo, according to the Sheriff's Department.

Detectives stayed with the boat while waiting for a towing ship and had planned to examine the boat for additional evidence, but the heavy surf caused the boat to break in two. The rear portion of the vessel sank about 40 feet offshore, and the Coast Guard started cleanup efforts. The large fuel tanks of the vessel and debris were recovered, but the boat itself remains in the water and is of no further value as evidence.

The Sheriff's Department said the outcome of the vessel is undetermined at this time.

The public is asked to be aware of the growing problem and to contact law enforcement if they see any suspicious boats in the ocean off Santa Barbara County. The U.S. Immigration and Customs Enforcement's toll-free 24-hour tip line can be reached at 866.DHS.2ICE.

A 30-foot Panga boat discovered Monday off the coast north of Refugio Beach by off-duty sheriff's deputies broke in two in heavy surf and sank. (Santa Barbara County Sheriff's Department photo)

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Florida Growers Brace For Cold Snap

By Doug Ohlemeier
The Packer
January 3, 2012

Florida grower-shippers are preparing for the season's first night of subfreezing temperatures.

Temperatures are forecast to fall as low as 23 degrees during the early morning hours of Jan. 4 in the Plant City, Fla., growing region, the hub for U.S. winter strawberries.

Ted Campbell, executive director of the Dover-based Florida Strawberry Growers Association, said growers plan to run irrigation to protect their berries from freezing temperatures. Beginning at 10 p.m. the evening of Jan. 3, growers plan to start spraying and finish by 9 a.m. when temperatures warm, Campbell said. He said this should be the first time cold weather could prompt growers to run irrigation.

"These plants have had it in luxury so far this season," Campbell said Jan. 3. "It's been in the 80s here. We may get lucky because there's not a lot of bloom exposure now. The plants are going into their normal rest after a heavy production of fruit. Tonight may coincide with that period."

Campbell said the spraying generally protects the berries and he hopes this cold snap won't be like last season when growers endured 10 consecutive nights of subfreezing temperatures. He said overnight temperatures are expected to increase the evening of Jan. 4 with temperatures forecast to rise to 70 degrees by the weekend of Jan. 7.

Earlier forecasts for the evening of Jan. 3 called for temperatures to fall to 29-31 degrees for Palm Beach County's sweet corn, green beans and lettuce production areas. However, forecasters changed that forecast to 34 degrees.

While the region is producing leafy greens and some beans remain in the ground, Bryan Biederman, assistant sales manager for Pioneer Growers Co-op, Belle Glade, Fla., said Pioneer's growers later in January plan to begin plantings for spring corn volume.

"If the wind can stay through the night, it will help with freezing temperatures," he said Jan. 3. "We're certainly not rooting for a freeze, but at this particular time in our corn planting schedule, We don't have a lot of corn in the ground."

Biederman called season growing conditions favorable.

Homestead, Fla., produces most of Florida's corn and beans in January and February.

Florida strawberry growers are bracing for low temperatures, including spraying water on plants, which provides a protective cover of ice.

[Return to top] *Topic Area: Agriculture and Food*

Daily Infectious Diseases Report - 04 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Infectious Diseases Report*

Daily Human Trafficking Report - 04 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Human Trafficking and Smuggling Report*

Daily Terrorism Report - 04 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Terrorism Report*

Daily Cyber Report - 04 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Cyber Report*

Daily Infrastructure Report - 04 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS IP Report*

UNCLASSIFIED

From: OSINT Branch Mailbox
To: OSINT Branch Mailbox
Subject: DHS-OSE Homeland Security Central Digest - 2012-01-12
Date: Thursday, January 12, 2012 6:46:06 AM
Attachments: DHS Daily Digest - 20120112.pdf

Classification: UNCLASSIFIED

(U) The DHS Homeland Security Central Digest for 12 January 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) Articles and resource documents come from open source information and are posted to the Homeland Security Central website on Intelink-U. For information on establishing an Intelink-U account, please visit http://ra.intelink.gov.

(U) The Homeland Security Central Digest contains full article text and may contain copyrighted material whose use has not been specifically authorized by the copyright owner. This information is available to DHS, in the interest of illuminating incidents and events that may have an impact on national security and critical infrastructure protection. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security

E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Digest
12 January 2012

County Seeks Eight-Year Sentence For Drug-Smuggling Pilot [PA]

A Colorado pilot will face at least eight years behind bars after he was convicted of charges he was involved in a plot to smuggle methamphetamine to the county. [HSEC-5.10]

US: Mexico Kingpin Joaquin 'El Chapo' Guzman Is 'World's Most Powerful Drug Trafficker'

The U.S. Treasury Department called Mexican drug lord Joaquin "El Chapo" Guzman "the world's most powerful drug trafficker" on Tuesday. [HSEC-5.10]

Orange Juice Fungicide Concern May Spike Prices

The Food and Drug Administration says it will step up testing for a fungicide that has been found in low levels in orange juice. [HSEC-6.2]

FDA Warns Of Mix-Up In Pills By Novartis

The Food and Drug Administration warned of potential mix-ups involving certain prescription pain pills and over-the-counter medicines that were made at a Novartis AG manufacturing plant in Nebraska. [HSEC-6.1]

Harvard Professor Addresses 2012 'Hacktivism' [MA]

In a talk given at Stanford Law School on Tuesday, Harvard Professor of Law and Computer Science Jonathan Zittrain expressed concern both over the Internet being too consolidated and controlled, as well as concern about security issues highlighted by "hacktivism" in 2011. [HSEC-1.10]

Feds Seek Stronger Security For Power Grid

Departments of Energy and Defense will create a cybersecurity model to test and apply across the utility industry, as they work to protect the U.S. electricity grid. [HSEC-1.9]

US Probes Alleged India Hacking Of Commission

US authorities have been asked to investigate allegations that hackers [in] India used back-door codes provided by companies to spy on private exchanges by a US commission on China, an official said Tuesday. [HSEC-1.10]

Trend Micro And Verizon Wireless Bring Mobile Security App To Millions Of Smartphone And Tablet Customers

The Latest Security Solutions from Trend Micro Offer New and Easy Ways to Secure Personal Information on Mobile Devices [HSEC-1.10]

2 Charged With Human Smuggling [TX]

A traffic stop for a dirty license plate led Buda police to two human smuggling suspects. [HSEC-3.10]

TSA Found Four Guns Per Day Last Year At Airports

Airport security officers found about four firearms per day at checkpoints last year and many of them were loaded, the Transportation Security Administration (TSA) said. [HSEC-10.9]

Full Text of all new articles....

County Seeks Eight-Year Sentence For Drug-Smuggling Pilot [PA]

By Carl Hessler Jr.
Montgomery News
January 10, 2012

A Colorado pilot will face at least eight years behind bars after he was convicted of charges he was involved in a plot to smuggle methamphetamine to the county.

Montgomery County First Assistant District Attorney Kevin R. Steele filed court papers Friday indicating he will seek at least an eight-year mandatory sentence against James Michael Handzus, 51, of Rifle, Colo., who was convicted in November of charges of possession with intent to deliver methamphetamine, criminal use of a communication facility, possession of drug paraphernalia and conspiracy in connection with incidents that occurred in April 2011 in Plymouth and at Wing's Field in Whitpain.

State law allows for certain mandatory prison sentences based on the amount of drugs involved in crimes. Because Handzus was convicted of possession with intent to deliver 433.6 grams of methamphetamine, prosecutors can seek the imposition of an eight-year mandatory sentence and a $50,000 fine, according to court documents.

Once prosecutors seek a mandatory sentence, judges have no discretion but to impose the punishment.

Handzus potentially could face even more prison time if a judge imposes consecutive sentences for the other crimes of which he was convicted. Judge Joseph A. Smyth, who convicted Handzus of the charges during a non-jury trial in November, is slated to sentence Handzus later this year.

Handzus remains in the county jail pending his sentencing hearing.

During the two-day trial, Steele argued the one pound of methamphetamine that was seized had a street value of between $64,000 and $76,800. Steele, who was assisted by prosecutor Lindsay Carfagno, characterized Handzus' arrest as a "significant drug bust."

Handzus' girlfriend, Tamara Vincent, 41, pleaded guilty to charges of possession with intent to deliver methamphetamine and conspiracy in connection with the incident and is also awaiting sentencing. Vincent's lawyer, John I. McMahon Jr., said Vincent participated in the conspiracy but was not the "main actor."

Vincent faces a possible maximum sentence of 10 to 20-years in prison on the charges.

Despite his girlfriend's admission, Handzus opted to go to trial on the charges, which were the culmination of a sting operation conducted by county detectives.

During his testimony, Handzus maintained he was set up by a police informant, claiming the informant planted the one pound of methamphetamine inside his luggage. Defense lawyer Douglas P. Earl argued prosecutors did not have sufficient evidence that Handzus planned to deliver the one pound of meth to detectives.

But prosecutors said detectives did an outstanding job investigating Handzus.

In March, the district attorney's Drug Task Force and Narcotics Enforcement Team, which had been investigating the distribution of methamphetamine in the county, learned that Handzus allegedly had been smuggling large quantities of methamphetamine into the county using his airplane, nicknamed "My Lady," according to arrest documents.

On April 21, authorities learned Handzus was arriving at Wing's Field in Whitpain, court papers indicate. Although Handzus did not file flight plans before piloting the aircraft on a 2,400 mile trip from Las Vegas, investigators had seen his Facebook page and learned of his travel plans, court records indicate.

After the Colorado couple was in town, an undercover detective arranged to purchase the meth from Handzus the following day, according to arrest documents. The undercover detective arranged to meet Handzus and Vincent at Ruby Tuesday's on Chemical Road in Plymouth, court papers indicate.

At the restaurant, Vincent allegedly explained that her boyfriend had family in the area, and when the couple visited they brought the drugs to sell to pay expenses and provide spending money, according to court papers. She allegedly agreed to sell the undercover detective a pound of meth for $27,000.

Vincent suggested the prospective buyer could divide the substance up into eighths of an ounce, called "eight balls," that would sell on the street for between $500 to $600 each, according to prosecutors. Selling the meth in those quantities would result in a street value between $64,000 and $76,800, authorities alleged.

After inspecting the meth, the undercover detective gave Vincent a $2,000 down payment. Detectives then moved in and arrested the couple, and the pound of "crystal meth" was seized from the couple's luggage, according to court documents.

Prosecutors previously alleged the methamphetamine was manufactured in Mexico and sent to Las Vegas, which is "the hub of distribution" for the illicit narcotic in the United States. Prosecutors described the confiscated drugs as "very high grade."

Authorities previously moved to take possession of the airplane, a 1959 Piper Comanche, under state drug forfeiture laws.

[Return to top] *Topic Area: Illegal Drug Trafficking*

US: Mexico Kingpin Joaquin 'El Chapo' Guzman Is 'World's Most Powerful Drug Trafficker'

MSNBC
January 11, 2012

The U.S. Treasury Department called Mexican drug lord Joaquin "El Chapo" Guzman "the world's most powerful drug trafficker" on Tuesday.

The fugitive Sinaloa cartel leader also got a boost from Mexican actress Kate Del Castillo, who said she believed in Guzman more than in the government.

It was the latest in an odd series of accolades for Guzman, who was included this year on the Forbes list of the world's richest people, with an estimated fortune of $1 billion.

The U.S. Embassy in Mexico City issued a statement saying three of Guzman's alleged associates had been hit with sanctions under the drug Kingpin Act, which prohibits people in the U.S. from conducting businesses with them and freezes their U.S. assets. The two Mexican men and a Colombian allegedly aided Guzman's trafficking operations.

The statement quoted Adam J. Szubin, director of the Treasury Department's Office of Foreign Assets Control, as saying the move "marks the fourth time in the past year that OFAC has targeted and exposed the support structures of the organization led by Chapo Guzman, the world's most powerful drug trafficker."

Bounty

Guzman, who escaped from a Mexican prison in 2001 in a laundry truck and has a $7 million bounty on his head, has long been recognized as Mexico's most powerful drug capo. Authorities say his Sinaloa cartel has recently been expanding abroad, building international operations in Central and South America and the Pacific.

Del Castillo, who played a female drug trafficker in the TV series "La Reina del Sur" ("Queen of the South"),

offered grudging praise for Guzman in a posting Tuesday on the social media site Twextra, linked to her Twitter account.

"Today, I believe more in El Chapo Guzman than in the governments who hide truths from me," she wrote.

The actress did not specify whether she was referring to the Mexican government, or what she meant when she accused "governments" of "hiding the cures for cancer, AIDS, etc. for their own benefit and enrichment."

Del Castillo's publicist, Marianne Sauvage, confirmed in an email to The Associated Press that the actress wrote the posting, and that the account belonged to Del Castillo.

'Positive things'

The 800-word posting ended with an impassioned plea to Guzman:

"Mr. Chapo, wouldn't it be great if you started trafficking with positive things? With cures for diseases, with food for street children, with alcohol for old people's homes so they spend their final days doing whatever they like, trafficking with corrupt politicians and not with women and children who wind up as slaves?"

"Go ahead, dare to, sir, you would be the hero of heroes, let's traffick with love, you know how," the message concluded.

Like late Colombian drug lord Pablo Escobar, Guzman has a reputation as a protector of his heartland in Sinaloa, a rugged region that the state still struggles to penetrate, where news of approaching of strangers quickly reaches him and his followers.

"Chapo has allegedly paid for schools, hospitals, and other public projects," his biographer Malcolm Beith told Reuters.

"Second, he's just about the only source of employment in parts of Sinaloa. And he has provided security of a sort. He's been known to apprehend small-time crooks or thugs when they got out of hand. Lastly, the name Chapo pretty much puts the fear of God into people."

With locals watching his back, Guzman has always had just enough warning to get away at the last minute. The exception was when soldiers captured him in Guatemala in June 1993.

[Return to top] *Topic Area: Illegal Drug Trafficking*

Orange Juice Fungicide Concern May Spike Prices

The Associated Press / CBS News
January 11, 2012

The Food and Drug Administration says it will step up testing for a fungicide that has been found in low levels in orange juice.

FDA officials said they aren't concerned about the safety of the juice but will increase testing to make sure the contamination isn't a problem. In a letter to the juice industry Monday, the agency said that an unnamed juice company contacted FDA in late December and said it had detected low levels of the fungicide carbendazim in the company's own orange juice and also in its competitors' juice. Fungicides are used to control fungi or fungal spores in agriculture.

Orange juice futures surged nearly 11 percent on Tuesday, gaining 20 cents to close at about $2.08 cents a pound. Investors are concerned that increased testing could pinch juice supplies. TransWorld Futures analyst Robert Rutger said the supply questions were enough to send prices higher, even though current inventories are relatively healthy.

Carbendazim is not currently approved for use on citrus in the U.S., but is used in Brazil, which exports orange juice to the United States. Brazil is the biggest producer of oranges in the world, according to the Agriculture

Department.

Top orange juice brands in the U.S. include PepsiCo's Tropicana and Minute Maid, marketed by The Coca-Cola Co. A Minute Maid spokesman declined to comment, referring questions to the Juice Products Association trade group. A spokeswoman for the association said the group had no comment ready by Tuesday evening.

An FDA spokeswoman said the company's testing found levels up to 35 parts per billion of the fungicide, far below the European Union's maximum residue level of 200 parts per billion. The U.S. has not established a maximum residue level for carbendazim in oranges.

In the letter to the Juice Products Association, FDA official Nega Beru said the agency will begin testing shipments of orange juice at the border and will detain any that contain traces of the chemical. Because it is not approved for use in this country, any amount found in food is illegal.

Beru said that because the FDA doesn't believe the levels of residue are harmful, and the agency won't remove any juice currently on store shelves. But he asked the industry to ensure that suppliers in Brazil and elsewhere stop using the fungicide.

"If the agency identifies orange juice with carbendazim at levels that present a public health risk, it will alert the public and take the necessary action to ensure that the product is removed from the market," he said.

The discovery comes after the agency said it would also step up testing for arsenic in apple juice. FDA officials said last year that the agency is considering tightening restrictions for the levels of arsenic allowed in the juice after consumer groups pushed the agency to crack down on the contaminant.

Studies show that apple juice has generally low levels of arsenic, and the government says it is safe to drink. But consumer advocates say the FDA is allowing too much of the chemical -- which is sometimes natural, sometimes man made -- into apple juices favored by thirsty kids.

Patty Lovera of the consumer group Food and Water Watch said the federal government needs to rely on its own testing, not that of the companies.

"The federal government needs to set consistent, meaningful, enforceable standards for all toxins," she said.

[Return to top] *Topic Area: Public Health & Healthcare*

FDA Warns Of Mix-Up In Pills By Novartis

By Jeniffer Corbett Dooren
The Wall Street Journal
January 10, 2012

The Food and Drug Administration warned of potential mix-ups involving certain prescription pain pills and over-the-counter medicines that were made at a Novartis AG manufacturing plant in Nebraska.

Novartis is recalling 1,645 lots of its Excedrin, NoDoz, Bufferin and Gas-X medicines because the products could contain stray capsules or caplets from other products, or "contain broken or chipped tablets."

The plant in Lincoln, Neb., where the products are manufactured was shut down last month. The plant also makes some opioid prescription painkillers for Endo Pharmaceuticals Holdings Inc., including Opana, Percocet and an extended-release version of morphine tablets.

Both Novartis and the FDA said they weren't aware of any adverse events in patients from any mix-ups. Novartis said it was offering customers a refund.

The company said Gas X Prevention is the only Novartis product manufactured on the same line as the Endo products and that it doesn't have any reports of any mix-ups of those medicines.

Novartis is the most recent company to suffer from production problems. Just last month Johnson & Johnson's

McNeil Consumer Healthcare unit recalled 12 million bottles of Motrin, saying some pills may not dissolve as quickly as intended. That company has been plagued by manufacturing quality problems since 2009 and has dozens of product recalls including Tylenol and Benadryl.

However, "given existing inventories, the expected restart of Novartis production and our ability to shift production to other facilities we believe the supply constraints of our products should be limited," said Julie McHugh, the company's chief operating officer.

Novartis said it would take a charge estimated at $120 million in the fourth quarter of 2011 related to the recalls and the work needed to fix the Lincoln facility.

"We are committed to a single quality standard for the entire Novartis Group and we are making the necessary investments and committing the right resources to ensure these are implemented across our entire network," Joseph Jimenez, the Swiss company's chief executive, said.

Edward Cox, a director in FDA's office of new drugs, said there's a potential for tablets to be retained in a machine involved in the product packaging process but said the FDA couldn't comment further on the ongoing investigation into the plant's problems.

Mr. Cox said the agency opted against asking for a recall of Endo's prescription pain products because the potential for drug mix ups appeared to be low and pharmacists can screen for any problems before the pain pills reach consumers. He said there's been three reports of mix-ups since 2009 that were caught by pharmacists. Endo on Monday said there may be a short-term disruption in the supply of some of its pain products and recommended that doctors refrain from starting new patients on the extended-release version of Opana to preserve supply for existing patients.

A July inspection report released by the FDA cited several consumer complaints of certain formulations of Excedrin being mixed up. For example some consumers said they found Excedrin Migraine Tablets being mixed with Excedrin Migraine caplets or geltabs. The agency said Novartis failed to adequately investigate 166 complaints related to "foreign tablets in your drug products since 2009."

Specifically Novartis is recalling three types of Bufferin, an aspirin product, and Gas-X Prevention, a food-enzyme supplement, with expiration dates of Dec. 20, 2013 or earlier. The company is recalling certain bottle sizes of its pain medicine Excedrin and NoDoz products with expiration dates of Dec. 20, 2014 or earlier. NoDoz contains caffeine and is marketed as an alertness product.

Detailed information about the recalled products can be found at www.novartisOTC.com.

Corrections & Amplifications
An earlier version of this article said the FDA warned of potential mix-ups of prescription pain pills and over-the-counter medicines like Excedrin and NoDoz made at a Novartis AG manufacturing plant in Nebraska, Late Monday, the company said that only Gas-X is produced on the same manufacturing line as the prescription drugs and that it doesn't have any reports of mix-ups in those medicines.

[Return to top] *Topic Area: Public Health & Healthcare*

Harvard Professor Addresses 2012 'Hacktivism' [MA]

By Josh Hoyt
The Stanford Daily
January 11, 2012

In a talk given at Stanford Law School on Tuesday, Harvard Professor of Law and Computer Science Jonathan Zittrain expressed concern both over the Internet being too consolidated and controlled, as well as concern about security issues highlighted by "hacktivism" in 2011.

The event, 'Hacktivism: Anonymous, Lulzsec and Cybercrime in 2012 and Beyond,' was sponsored by CodeX: The Stanford Center for Legal Informatics. CodeX is a multidisciplinary laboratory run by the University that seeks

"to explore ways in which information technology can be used to enhance the quality and efficiency of our legal system while decreasing its cost," according to its website.
Zittrain, co-founder and co-director of the Berkman Center for Internet & Society at Harvard, has often concerned himself with potentially harmful censorship and limits to freedom on the Internet, but in this talk, focused on one major drawback: major security concerns that are often beyond the skill level of the general public to comprehend and address.

"About a year ago it dawned on me that our information environment is one in which, if you anger the wrong people, your entire life is vulnerable," Zittrain said. "That is a high cost to pay for security, and it carries certain drawbacks that we shouldn't have to entertain."

Zittrain described fears over the worst-case scenario cyber attacks getting the bulk of public attention — like an attack that disables the power grid or interferes with a nuclear plant. He addressed such scenarios as real, but the product of "hype."

Instead he singled out attacks like distributed denial of service attacks (DDoS), which were at the center of many important news stories in 2011, including attacks on governments in the Middle East and on companies that had severed ties with WikiLeaks.

Zittrain related how Anonymous, a loose Internet group known for activist hacking, retaliated against HB Gary Federal, an Internet security consulting firm, and its CEO Aaron Barr. Aaron Barr had his Twitter and Facebook hacked to announce his home address and social security number. Additionally, all of the internal company emails were hacked and released.

Ultimately, Anonymous itself was compromised and forced to announce: "We regret to inform you today that our network has been compromised by a former IRC-operator and fellow helper named 'Ryan.'"

"I don't know if you've seen Reservoir Dogs where everybody is pointing their guns at each other," Zittrain said. "But this is where I say 'things have gone too far.'"

Everybody is vulnerable in this environment, including expert consultants in cyber security, according to Zittrain.

"This box in front of me [pointing at his laptop] contains all of my emails on it, and if Anonymous were mad enough at me, I have every confidence that they would be in this box within 12 hours," Zittrain said. "Maybe if I broke it over my knee and never plugged it in again…" he joked.

Zittrain did not offer any specific solutions to the balance, but he favors a solution that would be "bottom up" in nature, not a government-driven solution. He looks to models like Wikipedia for bottom-up governance that works. Zittrain acknowledged that any solution would have to work with the nature of the consumers.

"How do we build systems that are still extremely simple and intuitive to use, but capture experimentalist spirit that was so important to the development of the Internet?" Zittrain asked.

Zittrain will not have to come up with all of the answers himself, as students in a Law class called 'Ideas for A Better Internet' attended the event. The class has students from both Stanford and Harvard who will be presenting their work in an event on Wed., Jan. 18.

Eli Marschner, a second-year graduate student in computer science, is working on the issues related to journalism on the Internet. He came away from this talk pondering the differences between online activism and traditional activism.

"With online civil disobedience, if you want to call it that, it is not highly organized groups who are dedicating their time and risking being arrested," Marschner said. "It might be somebody in their basement running downloaded software their friend told them to download. The scale is fundamentally different."

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Feds Seek Stronger Security For Power Grid

By Elizabeth Montalbano
InformationWeek
January 10, 2012

The Department of Energy (DOE) and the Department of Defense (DHS) have teamed up to create a cybersecurity model that can be tested and applied across the utility industry to provide insight into how to better protect the U.S. electricity grid.

The Electric Sector Cybersecurity Risk Management Maturity Model pilot project aims to work with experts in both the public and private sector to use existing cybersecurity strategies to develop a so-called "maturity model" that can identify how secure the electricity grid currently is from cyber threats, according to a White House blog post by White House cybersecurity coordinator Howard Schmidt. It will then test that model with participating utility companies to see how well it works, he said.

Maturity models use best practices to identify strengths and weaknesses in an organization or system, and are used by industry sectors to improve performance, efficiency, and quality.

"Gaining knowledge about strengths and remaining gaps across the grid will better inform investment planning and research and development, and enhance our public-private partnership efforts," Schmidt said.

The DOE is taking the lead on the project, with help from the DHS. Over the next few months, the DOE will host workshops with the private sector to draft a maturity model for the electricity industry. That model will be tested across the more than a dozen electric utilities and grid operators that are expected to participate in the pilot program, and a risk-management model will be released to the electricity sector later this summer.

The Obama administration has put a particular focus on protecting the electricity grid and other control systems from a persistent and growing cybersecurity threat, and patterning with the private companies that control that sector has been key to the effort.

Indeed, if viruses such as the Stuxnet and Duqu are any indication, hackers now are designing threats to explicitly attack control systems, which has not only the feds but other government leaders around the world on alert about how to protect these critical systems.

The new DOE-DHS project itself grew out of previous work federal officials have done to examine the threat to the electricity grid. Cybersecurity is one of four key themes of the administration's Policy Framework for a 21st Century Grid, released last June. Two months later, the DOE released the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity, an update to a similar document produced in 2006. The earlier document outlined a strategic framework to be implemented over the next decade to create and operate a resilient energy system that can recover in the case of a major cyber incident.

[Return to top] *Topic Area: Energy*

US Probes Alleged India Hacking Of Commission

AFP
January 10, 2012

US authorities have been asked to investigate allegations that hackers [in] India used back-door codes provided by companies to spy on private exchanges by a US commission on China, an official said Tuesday.

A hacker group calling itself the Lords of Dharmaraja released excerpts of documents that it said were part of an Indian intelligence unit's surveillance of the US-China Economic and Security Review Commission.

"We are aware of these reports and have contacted relevant authorities to investigate the matter," commission spokesman Jonathan Weston said. He declined further comment.

The commission, which consists of 12 experts, was set up by Congress in 2000 to monitor the security implications of US trade with China. It publicly releases findings and recently produced an extensive study on

alleged Chinese cyber-espionage.

The email exchanges released by the hackers showed the commissioners discussing their wording on issues such as arms sales to Taiwan and China's currency valuation but did not appear to contain bombshells.

However, a purported document on Indian military letterhead states that spies were able to access the exchanges through a "backdoors" method made available to Indian authorities by communication companies.

"Decision was made earlier this year to sign an agreement with mobile manufacturers in exchange for the Indian market presence," said the alleged document dated October 6.

It specifically names BlackBerry smartphones' Canadian maker Research In Motion (RIM), US tech giant Apple and Finnish mobile manufacturer Nokia.

It was not possible to verify independently the authenticity of the document, which unclearly speaks of authorization for the operation by "the President."

Representatives from the companies and the Indian embassy in Washington did not immediately respond to requests for comment.

India a year ago resolved a prolonged standoff with RIM after authorities complained that terrorists could use encrypted BlackBerry messages.

BlackBerry said in January 2011 it would allow the Indian government to monitor BlackBerry messenger and public email services, but not corporate emails.

India has uneasy relations with fellow Asian giant China. India recently lodged a protest after two of its nationals alleged that they were tortured in a hotel room over a business dispute in the city of Yiwu.

Relations also remain tense over a border dispute and India's welcoming of thousands of Tibetans who fled Chinese rule, including the Dalai Lama.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Trend Micro And Verizon Wireless Bring Mobile Security App To Millions Of Smartphone And Tablet Customers

Sacramento Bee
January 11, 2012

From the 2012 International Consumer Electronics Show (CES), Verizon Wireless and Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, today announced Trend Micro™ Mobile Security Personal Edition is now available in Verizon Apps on select Verizon Wireless Android™ devices. The app will be demonstrated at the Verizon booth (Las Vegas Convention Center, South Hall, Booth #30259) throughout the show.

Trend Micro Mobile Security Personal Edition for Android addresses a need for cyber security on mobile devices and offers an easy solution for Verizon Wireless customers to help keep personal information on their Android devices safe.

After downloading the app, customers can take advantage of key features, including an app scanner, lost device protection and enhanced security to block threats as well as inappropriate content while surfing the Web, calling or texting.

"Smartphones are a key form of communication today and contain the type of irreplaceable personal information hackers find most valuable. This is why we're excited to be able to offer Verizon Wireless' customers an application that can protect their personal information, keep their kids safe online and help recover a lost device," said Carol Carpenter, general manager, Consumer Division at Trend Micro.

Verizon Wireless' mobile storefront, Verizon Apps (formerly V CAST Apps), is available on select smartphones and delivers thousands of apps and games to Verizon Wireless customers. Powered by the Verizon Developer Community (VDC), Verizon Apps enables customers to discover, purchase and use apps with a simple process and offers the ease and convenience of direct billing – apps purchased are invoiced on customers' monthly bills.

Customers can download Trend Micro Mobile Security Personal Edition from Verizon Apps in the Utilities category. Trend Micro Mobile Security Personal Edition offers Verizon Wireless customers anti-malware app scanning for free with premium features available for a $2.50 monthly subscription or $30 per year on a number of popular Verizon Wireless 3G devices, including DROID Incredible 2 by HTC, DROID X2 by Motorola, CASIO® G'zOne® Commando, and on several 4G LTE smartphones, including ThunderBolt™ by HTC, Revolution™ by LG and DROID Charge by Samsung. Data charges may apply when browsing, downloading and using certain applications.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

---

2 Charged With Human Smuggling [TX]

KXAN
January 10, 2012

A traffic stop for a dirty license plate led Buda police to two human smuggling suspects.

The officers stopped a pickup truck last month on Interstate Highway 35 because it had a mud-covered plate. They found three people concealed in the car.

Officers arrested Fermin Rubio, 18, and Robert Trevino, 19, both from Carrizo Springs. They are charged with human trafficking, a second-degree felony. Both men were released on $10,000 bond each.

The men who were hiding told police they paid $100 to Rubio for a ride.

Police said the pair was taking illegal immigrants from a home near the Mexican border to safe house in Dallas.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

TSA Found Four Guns Per Day Last Year At Airports

Reuters
January 10, 2012

Airport security officers found about four firearms per day at checkpoints last year and many of them were loaded, the Transportation Security Administration (TSA) said.

TSA personnel found 1,238 firearms at security checkpoints in 2010, up 54 percent from 2007, according to agency data.

Many of the weapons were found loaded with rounds in the chamber. Most passengers said they forgot they had a gun in their bag, according to a TSA blog on 2011 highlights.

In one week this year, agents found 14 loaded and five unloaded handguns in carry-on luggage, according to another TSA blog.

They also have discovered a speargun, a live teargas grenade, inert hand grenades and four knives in a single bag.

A TSA spokesman declined to comment on a reason for the increased number of firearms.

TSA Administrator John Pistole told Congress in November: "Clearly just the fact that we are getting four to five guns every day indicates that there are people who are not focused on the security protocols."

(Reporting by Ian Simpson; Editing by Greg McCune)

[Return to top] *Topic Area: Airports & Airlines*

Daily Infectious Diseases Report - 11 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Infectious Diseases Report*

Daily Human Trafficking Report - 11 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Human Trafficking and Smuggling Report*

Daily Terrorism Report - 11 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Terrorism Report*

Daily Cyber Report - 11 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Cyber Report*

Daily Infrastructure Report - 11 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS IP Report*

UNCLASSIFIED

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Homeland Security Central Digest - 2012-01-27
Date:	Friday, January 27, 2012 7:09:51 AM
Attachments:	DHS Daily Digest - 20120127.pdf

Classification: UNCLASSIFIED

(U) The DHS Homeland Security Central Digest for 27 January 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) Articles and resource documents come from open source information and are posted to the Homeland Security Central website on Intelink-U. For information on establishing an Intelink-U account, please visit http://ra.intelink.gov.

(U) The Homeland Security Central Digest contains full article text and may contain copyrighted material whose use has not been specifically authorized by the copyright owner. This information is available to DHS, in the interest of illuminating incidents and events that may have an impact on national security and critical infrastructure protection. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6) .

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security

E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Digest
27 January 2012

Human Smuggling Suspects Caught Near Nevada State Line [AZ]

Authorities arrested two suspected human smugglers believed to have been transporting six illegal immigrants just past the Nevada-Arizona border. [HSEC-3.10]

Feds: US Terrorist Took Out Murder Contract On Witnesses [NC]

A man already convicted of taking part in a terror plot to attack the U.S. Marine Corps base in Quantico, Virginia has now been accused of plotting the beheading of key witnesses against him and his co-conspirators. [HSEC-8.10]

SCADA Systems In Railways Vulnerable To Attack

Reports of a possible cyber-attack against a rail company highlight the issues of protecting industrial control systems that keep the country's critical infrastructure running. [HSEC-1.1]

AP Interview: Saudi Royal Warns That Mideast Could Face Nuclear Arms Race

An influential member of the Saudi royal family warned Wednesday that unless the Middle East becomes a nuclear weapon-free zone, a nuclear arms race is inevitable and could include his own country, Iraq, Egypt and even Turkey. [HSEC-10.3]

20 People Arrested, 24 Pounds Of Meth Seized In Drug Bust [WA]

A massive, multi-jurisdictional investigation into drug trafficking that crossed several states and at least two countries ended Wednesday with the arrests of 20 alleged drug dealers. [HSEC-5.10]

Zetas Now Mexico's Biggest Cartel, Report Says

The Los Zetas cartel has supplanted the Sinaloa mob as Mexico's largest drug-trafficking organization in terms of geographic presence, security consulting firm Stratfor said in a report. [HSEC-5.2]

Federal Agents Bust Alleged Aircraft Smuggling Operation [CA]

While smugglers often use ultralight planes to bring drugs across the U.S-Mexico border, the use of private aircraft is rare. Yet, federal agents east of San Diego County say they've seized a Cessna plane in an alleged human smuggling operation. [HSEC-3.10]

Foods To Beat The Winter Blues

Day after day of gray skies and cold weather, and you just might find yourself coming down with a case of the winter blues. [HSEC-6.2]

FTC Site Still Down After Anonymous Hack; Anti-Piracy Fallout Spreads

The Federal Trade Commission's cybersecurity advice website remained offline Jan. 25, a day after it had been

hacked by the group Anonymous in a continuing protest over proposed anti-piracy laws and recent anti-piracy arrests. [HSEC-1.10]

Ex-UCF Student Pleads Guilty To Federal Hacking Charge [FL]
A now former University of Central Florida student charged with hacking into a website used by the FBI recently pleaded guilty in federal court, records show. [HSEC-1.10]

Bizarre Skin Disease Morgellons Not Infectious, CDC Says
After an exhaustive search, researchers at the Centers for Disease Control and Prevention have found no sign of an infectious agent, parasite or environmental exposure that could explain the mysterious skin condition known as Morgellons disease. [HSEC-6.2]

Many Pediatric ICUs Have High Infection Rates
Infections in pediatric intensive care units put children's lives at risk and occur all too often, according to a new investigation from the Consumer Reports Health Ratings Center. We found that pediatric ICUs often have higher infection rates than adult ICUs, and that some hospitals do much better than others at preventing infections. [HSEC-6.2]

Two Accused Of Trying To Smuggle Illegal Aliens To Ohio
Mohave County Sheriff's deputies arrested two Maryland cousins near Littlefield on human smuggling charges, an MCSO spokeswoman said Wednesday. [HSEC-3.10]

Full Text of all new articles....

Human Smuggling Suspects Caught Near Nevada State Line [AZ]

By Matt Guillermo
Fox 5 Vegas
January 25, 2012

Authorities arrested two suspected human smugglers believed to have been transporting six illegal immigrants just past the Nevada-Arizona border.

According to the Mohave County, Ariz. Sheriff's office, deputies pulled over a vehicle around 11 p.m. Sunday on Interstate 15 at mile marker 22 near the town of Littlefield, which is 10 miles east of Mesquite.

Deputies determined six occupants in the vehicle were illegal immigrants and Border Patrol agents took them into custody, deputies said.

Officers also determined that the driver, Henrry Leon-Zacarias, 29, and a passenger, Erwin Zacarias-Leon, 24, both of Maryland, were transporting the illegal immigrants to Ohio

Authorities arrested both men on felony human smuggling and unlawful transport of aliens charges.

The two men were booked into the Mesquite Jail. The illegal immigrants were transported to the Washington County, Utah Jail where Border Patrol took them into custody.

The Mohave County Sheriff's office did not disclose why deputies stopped the vehicle.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Feds: US Terrorist Took Out Murder Contract On Witnesses [NC]

By Jason Ryan, Pierre Thomas and Jack Cloherty
ABC News
January 25, 2012

A man already convicted of taking part in a terror plot to attack the U.S. Marine Corps base in Quantico, Virginia has now been accused of plotting the beheading of key witnesses against him and his co-conspirators.

According to a criminal complaint unsealed this week, Hysen Sherifi tried to arrange for the witnesses to be murdered for $5,000 apiece by a hitman named "Treetop," but the go-betweens in the murder-for-hire scheme were actually federal informants.

Hysen Sherifi was convicted of providing material support to terrorists, conspiracy to murder U.S. military personnel and firearms charges in October 11 for his role in the foiled Quantico plot. Three other men in his North Carolina-based terror cell pled guilty to terrorism charges in 2011, and three more defendants were found guilty at trial. Another defendant still awaits trial, while an eighth suspect remains at large.

Sherifi, 27, was sentenced to 45 years in federal prison on January 13. In an FBI affidavit unsealed this week, however, authorities claim that prior to Sherifi's sentencing he tried to take out a murder contract on key witnesses against him.

According to the affidavit, Sherifi confided in an informant that he wanted to kill three witnesses who testified against him and a prisoner he believed had stolen from him.

"[The Informant] contacted the FBI to advise that Hysen Sherifi had confided in him and requested his/her assistance for the purpose of hiring someone to kill several individuals. Three of the intended victims are witnesses who testified against him at his federal trial."

The affidavit alleges that Sherifi showed his brother's girlfriend, Nevine Aly Elshiekh, notes that he wanted passed on to another individual who was also an informant in the case.

Elshiekh allegedly passed the information on to the second informant, who claimed to be in contact with a hitman known only as "Treetop." During a January 2, 2012 meeting the second informant allegedly showed Elshiekh a picture of one of the targets and the two discussed a $5,000 payment for the killings. "I got the picture from Treetop," the informant allegedly told Elshiekh, "and Treetop wants to make sure it's the right person to be killed."

On Jan. 8, 2012, Sherifi's brother Shkumbin Sherifi visited his brother at the New Hanover County jail. Two hours later, Shkumbin allegedly arranged a call with the second informant to meet him and get money to him. The court papers note that Shkumbin Sherifi allegedly brought the informant $4,250.

During the meeting the informant allegedly asked Shkumbin Sherifi, "You need to ask [Hysen] Sherifi which one he want [sic] killed. The black guy or Arab."

Shkumbin allegedly told the informant 'Okay, um does he, um, are you guys in touch?"

The court documents note that Shkumbin "claimed not to know what was going on but promised to speak with his brother and get a response."

Shkumbin Sherifi and Elshiekh are charged in the alleged murder-for-hire plot and are scheduled to have a detention hearing in Wilmington, N.C., on Friday. Hysen Sherifi has not yet been charged. The brothers are natives of Kosovo and emigrated with their family to the U.S. in the 1990s.

[Return to top] *Topic Area: Terror Investigations and Trials*

SCADA Systems In Railways Vulnerable To Attack

By Fahmida Y. Rashid
eWeek.com
January 25, 2012

Reports of a possible cyber-attack against a rail company highlight the issues of protecting industrial control systems that keep the country's critical infrastructure running.

Government officials initially believed railway signal disruptions in December were tied to a cyber-attack against a Northwest rail company in December, Nextgov reported. But government and railway officials later denied that a U.S. railroad had actually been hit by a cyber-attack.

"There was no targeted computer-based attack on a railroad," said Holly Arthur, a spokeswoman for the Association of American Railroads.

While an attack has been ruled out, the incident highlights the dangers of industrial control systems controlling critical infrastructure.

Train service on the unnamed railway was "slowed for a short while" and schedules delayed for 15 minutes on Dec. 1, according to a Transportation Security Administration memo obtained by Nextgov. A "second event" occurred just before rush hour the next day, but it did not affect schedules, according to the Dec. 20 memo, which summarized the agency's outreach efforts to share threat intelligence with the transportation sector.

"Amtrak and the freight rails needed to have context regarding their information technical centers," the memo said, adding that rail operators were not focused on cyber-threats.

TSA investigators discovered two IP addresses for the intruders associated with the Dec. 1 incident and another for Dec. 2. Investigators considered the possibility of the attackers being based overseas, but did not specify the suspected country, Nextgov reported. Alerts listing the three IP addresses were sent to several hundred railroad firms and public transportation agencies.

Officials at the Department of Homeland Security, which oversees the TSA, told Nextgov on Jan. 23 that further investigation showed it may not have been a targeted attack, but did not explain what may have caused the "anomalous activity."

The railway incident is similar to what happened at an Illinois utility last fall. A government fusion center claimed Russian attackers had remotely destroyed the facility's water pump, but the DHS on further investigation claimed it was not an attack. It later turned out the intrusion had been an American contractor remotely logging in to perform some maintenance tasks.

However, the TSA's railway memo highlights how vulnerable the railways are to an attack on supervisory control and data acquisition (SCADA) systems, according to experts from Casaba Security, a security analysis and consulting company. Just about anything in the railway infrastructure could be controlled by SCADA systems, including track switches, signal and crossing lights, transformers, weather and track sensors, engine monitors, railway car sensors, electronic signs and even turnstiles, said Samuel Bucholtz, Casaba's co-founder. Most of these systems are connected to the network so that they can obtain data collected by the sensors.

"A sensor that can detect the position of a track switch is not helpful unless it can pass that data to an operations center hundreds of miles away," Bucholtz said.

Connecting SCADA systems to the Internet puts the infrastructure at risk because it opens up the possibility of intruders finding a way into the network. However, many organizations take that risk to save money, simplify the infrastructure and ease maintenance. It is usually cheaper to transmit data over the Internet instead of investing in dedicated lines or wireless frequency space, according to Bucholtz.

"The benefit of SCADA being 'online' is that the Internet is cheap, robust, standardized and easily accessible," Bucholtz said.

The downside is that without proper protections, the infrastructure is wide open to anyone looking. Cambridge University researcher Eireann Leverett developed a tool that mapped more than 10,000 industrial control systems accessible from the Internet, including water and sewage plants. While some of the systems could have been demo systems or used in places that wouldn't count as critical infrastructure, such as the heating system in office buildings, some were active systems in water facilities in Ireland and sewage facilities in California.

Only 17 percent of the systems mapped asked for authorization to connect, suggesting that administrators either weren't aware the systems were online or had not installed secure gateways, Leverett said. Leverett, a computer science doctoral student at Cambridge, presented the findings at the S4 conference in Miami.

Administrators need to set up secure and isolated networks and use Secure Sockets Layer or a virtual private network to restrict who can talk to the controllers, according to John Michener, chief scientist at Casaba. Since SCADA systems will likely be Internet-accessible, administrators should focus on putting them behind a secure gateway. "Increasingly all the communications are over the Net, so being on the Net is all but inescapable," Michener said.

[Return to top] *Topic Area: Rail & Mass Transit*

AP Interview: Saudi Royal Warns That Mideast Could Face Nuclear Arms Race

The Associated Press / The Washington Post
January 25, 2012

An influential member of the Saudi royal family warned Wednesday that unless the Middle East becomes a nuclear weapon-free zone, a nuclear arms race is inevitable and could include his own country, Iraq, Egypt and even Turkey.

Prince Turki Al Faisal said the five permanent U.N. Security Council members should guarantee a nuclear security umbrella for Mideast countries that join a nuclear-free zone — and impose "military sanctions" against countries seen to be developing nuclear weapons.

"I think that's a better way of going at this issue of nuclear enrichment of uranium, or preventing Iran from acquiring weapons of mass destruction," the former Saudi intelligence chief and ambassador to the U.S. and Britain said in an interview with The Associated Press. "If it goes that route, I think it's a much more equitable procedure than what has been happening in the last 10 years or so."

Turki said establishing a nuclear weapons-free zone "deserves everybody's attention and energy, more so than other activities which we see unfolding, whether it is redeployment of fleets in the area, whether Iranian or American or British or French, whether it is the sanctions efforts against Iran."

The Security Council has imposed four rounds of sanctions against Iran, mainly targeting its defense and nuclear establishment, but Tehran has refused to suspend uranium enrichment and enter negotiations on its nuclear activities. It maintains its nuclear program is peaceful, aimed solely at producing nuclear energy, but the U.S. and many European nations believe Iran's goal is to produce nuclear weapons.

Turki's proposal could impose sanctions against Iran if there is evidence it is pursuing weapons of mass destruction, which include nuclear as well as chemical and biological weapons. But it could also put Israel under sanctions if it doesn't come clean on its suspected nuclear arsenal.

Israel is widely believed to have an arsenal of hundreds of nuclear weapons but has avoided confirming or denying their existence.

An Arab proposal for a weapons of mass destruction-free zone was initially endorsed by the 1995 conference reviewing the Nuclear Nonproliferation Treaty, but never acted on.

In May 2010, the 189 member nations that are party to the NPT called for convening a conference in 2012. Last October, the U.N., U.S., Russia and Britain announced that Finland will host the conference this year.

Israel is not a party to the NPT and has long said a full Arab-Israeli peace must precede such weapons bans. But at the 2010 NPT review conference, the United States, Israel's most important ally, said it welcomed "practical measures" leading toward the goal of a nuclear-free zone in the Middle East.

It remains unclear, however, whether the U.S. or veteran Finnish diplomat Jaakko Laajava, who is serving as "facilitator" of this year's conference, can persuade Israel to attend.

Turki said his answer to American and British diplomats who say Israel won't accept a nuclear weapons-free zone is "So what?"

He said the five permanent members should make an announcement on the establishment of a Mideast zone free of weapons of mass destruction, or WMD, at this year's conference in Finland.

Turki cautioned, however, that actually establishing a WMD-free zone will take negotiations in which all the underlying issues in the region, from the establishment of a Palestinian state to the future of the Golan Heights, "will have to be dealt with to make the zone workable."

"So there are incentives there for everybody to be serious about establishing an overall peace so the zone can be put in place," he said.

Turki warned that if there is no WMD-free zone in the Mideast, "inevitably" there is going to be a nuclear arms race "and that's not going to be in the favor of anybody."

The Gulf states are committed not to acquire WMD, he said. "But we're not the only players in town. You have Turkey. You have Iraq which has a track record of wanting to go nuclear. You have Egypt. They had a very vibrant nuclear energy program from the 1960s. You have Syria. You have other players in the area that could open Pandora's box."

Asked whether Saudi Arabia would maintain its commitment against acquiring WMD, Turki said: "What I suggest for Saudi Arabia and for the other Gulf states ... is that we must study carefully all the options, including the option of acquiring weapons of mass destruction. We can't simply leave it for somebody else to decide for us."

[Return to top] *Topic Area: Nuclear Weapons*

---

20 People Arrested, 24 Pounds Of Meth Seized In Drug Bust [WA]

KOMONews.com
January 25, 2012

A massive, multi-jurisdictional investigation into drug trafficking that crossed several states and at least two countries ended Wednesday with the arrests of 20 alleged drug dealers.

Investigators say the 20 people now in custody are part of a drug ring that brought cocaine, methamphetamine and heroin from the San Francisco Bay Area into Seattle. The drugs were then distributed in western Washington or sent to Canada, according to the US Attorney's Office.

After an extensive investigation that involved wire taps of thousands of drug-related conversations, on Wednesday DEA agents and police executed search warrants on 18 residences, businesses and vehicles.

During those raids, they found 24 pounds of meth, powder cocaine and crack cocaine, along with $35,000 in cash.

"Today, over 24 pounds of methamphetamine was seized from one vehicle in this investigation, which has an estimated street value of over $1 million," said DEA Special Agent in Charge Matthew G. Barnes. "This investigation illustrates the defendants' ill-will and disregard for our community."

Over the course of the entire investigation, law enforcement officers seized more than $700,000 in cash, 11 kilos of cocaine, 40 pounds of meth and four firearms.

Investigators believe 38-year-old Jose Rodriguez-Rivera of Lynnwood is the ringleader of the group. Police searched his home, as well his cars -- a 2007 Pontiac G5, 2003 Hummer H2 and 2006 BMW 330 -- during the raid.

Court documents show that Rodriguez-Rivera has been under investigation since October, 2008.

"Organizations that think we cannot track their crimes across borders are wrong. We will use all of our tools to shut down their operations and seize their profits," said U.S. Attorney Jenny A. Durkan. "I commend the tremendous collaboration by federal, state and local law enforcement in disrupting this drug ring."

The defendants were arrested in Lynnwood, Federal Way, Sedro-Woolley, Everett, Seattle, Mountlake Terrace, Kent, Kirkland, Des Moines and Edmonds.

They've been charged with various federal crimes, including conspiracy to distribute controlled substances and/or conspiracy to engage in money laundering.

[Return to top] *Topic Area: Illegal Drug Trafficking*

Zetas Now Mexico's Biggest Cartel, Report Says

FOX News Latino
January 26, 2012

The Los Zetas cartel has supplanted the Sinaloa mob as Mexico's largest drug-trafficking organization in terms of geographic presence, security consulting firm Stratfor said in a report.

At the close of 2011, Los Zetas operated in 17 states, or more than half the country, while its rival had operations in 16 states, Stratfor said, citing a report by organized-crime prosecutors.

Unlike the Sinaloa cartel, which tends to use bribery to achieve its aims, the Zetas "prefer brutality ... intimidation and violence," according to report published Tuesday.

Stratfor noted that "with a leadership composed of former special operations soldiers, (Los Zetas) are quite effective in employing force and fear to achieve their objectives."

The Zetas, whose stronghold is northeastern Mexico, moved last year into the central state of Zacatecas and the northwestern state of Durango, "achieving a degree of control of the former and challenging the Sinaloa Federation in the latter."

They also began to establish control over the Pacific coast state of Colima and its coveted port of Manzanillo.

In contrast to the alliances Sinaloa forms with other cartels, Los Zetas' ties with other gangs tend to be "more fleeting," the report said.

Despite losing 17 of its cell leaders and heads of plazas (drug-smuggling corridors) in 2011 to death or arrest, Los Zetas remained powerful and continued to be the dominant force in the Yucatan Peninsula, Stratfor said.

The Sinaloa cartel, meanwhile, lost at least 10 plaza bosses or top lieutenants last year, although Stratfor said it is unclear how those setbacks affected the cartel's operations overall.

The Texas-based security consulting firm did note, however, that a government crackdown had affected the methamphetamine business of the Sinaloa mob, the dominant producer of that synthetic drug following the disintegration of the La Familia Michoacana crime syndicate in early 2011.

According to the report, drug-related homicides declined last year in some areas - notably in Ciudad Juarez, Mexico's murder capital - but rose in other places, including the cities of Veracruz, Monterrey, Matamoros and Durango.

In 2012, Stratfor predicts "more signs of Mexican cartel involvement in the Caribbean, Europe and Australia" due to the growing difficulty of smuggling cocaine into the United States.

Los Zetas used to serve as the armed wing of the Gulf mob, which the Stratfor report said has split into two factions and is weaker than before but "seems to have maintained control of its primary plazas ... into the United States."

The government said earlier this month that 12,903 people were killed in drug-related violence between January and September 2011 in Mexico, an increase of 11 percent from the same period in the prior year.

The drug war death toll stood at 47,515 from December 2006, when President Felipe Calderon took office and

militarized the struggle against the country's heavily armed drug mobs, to Sept. 30, 2011.

The murder total has grown every year since Calderon was inaugurated.

Unofficial tallies published in December by independent daily La Jornada put the death toll from Mexico's drug war at more than 50,000.

[Return to top] *Topic Area: Illegal Drug Trafficking*

Federal Agents Bust Alleged Aircraft Smuggling Operation [CA]

By Marissa Cabrera
KPBS.org
January 25, 2012

While smugglers often use ultralight planes to bring drugs across the U.S-Mexico border, the use of private aircraft is rare. Yet, federal agents east of San Diego County say they've seized a Cessna plane in an alleged human smuggling operation.

Immigration and Customs Enforcement (ICE) officials said they stopped the plane at the Imperial County Airport last Friday.

On board were three undocumented immigrants, two women and a man, along with a pilot.

The pilot, Lino Rodriguez 30, is a U.S citizen and has been charged with federal human smuggling charges. He pleaded not guilty to the charges Tuesday.

Ricardo Sandoval, assistant special agent in charge of ICE in El Centro, said the plane was headed to Hemet, about 80 miles north of San Diego. The pilot was apparently trying to avoid Border Patrol checkpoints along the way, said Sandoval.

Agents have caught four planes in connection with human smuggling in Imperial County during the last two years.

A spokesperson for the San Diego sector of the Border Patrol said there have been human smuggling cases involving aircraft in the last couple of years.

Friday's bust in Imperial County is part of an ongoing investigation.

Sandoval said ICE had been conducting surveillance on the migrants from the time they crossed the border in downtown Calexico.

"The investigation involves six illegal immigrants, who crossed on foot at the port of entry," he said.

Before heading to the airport, Sandoval said they stopped at a stash house and a Motel 6 in El Centro.

"At the hotel, three of them were seen heading to the airport," he said.

Sandoval said smuggling fees ranged from $2,500 to $5,000 each.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Foods To Beat The Winter Blues

By Tanya Zuckerbrot
Fox News
January 26, 2012

Day after day of gray skies and cold weather, and you just might find yourself coming down with a case of the

winter blues. The winter doesn't only affect the way we feel, but it also can change the way we eat. You may reach for calorie-laden comfort foods to boost your spirits, but in the end the weather is still bad and you feel overstuffed. Of nearly two thirds of U.S. adults, 64 percent agree that they are filled with greater joy soaking up the summer sun, then bundling up in winter coats. According to studies done at Cornell University, the winter blues and its more severe foil, Seasonal Affective Disorder (SAD), affects about four times as many women as men.

Research has begun to reveal how mindful eaters can choose their fuel to help achieve or maintain a desired mental state. The food you eat can also brighten your winter. Our moods are linked to the production or use of certain brain chemicals, and scientists have identified many of the natural chemicals in foods that change the way we feel. That's right, you can eat certain foods in order to beat the winter blues. Food influences neurotransmitters by attaching to brain cells and changing the way they behave. This opens pathways to those cells, so that other mood-altering chemicals can come through the gates and attach themselves to brain cells.

The next time bad weather has got you down take a walk to the kitchen! Here are the foods to eat to beat the winter blues:

When you want to feel pleasant and alert: Eating foods that stimulate the release of dopamine may produce enjoyable feelings. Phenylnine is an essential amino acid found in the brain and blood that can convert in the body to tyrosine, which in turn is used to synthesize dopamine, instantly increasing your energy and alertness. Start your morning off with eggs and whole wheat toast, which stimulate dopamine production, and will help keep you feeling energized throughout the day. Breakfast is a must because it provides glucose to your brain, making you mentally efficient and alert.

To ease feeling of depression: Eat more fish! Omega-3 fatty acids (found in fatty fish such as salmon, herring, sardines and tuna) may help ease depressive symptoms. People with higher blood levels of these fatty acids were reported to experience less depressive symptoms, and were generally found to be more pleasant. This effect may be attributed to the fact that omega-3 fats make up about 8 percent of our brain. Higher intakes of these fats are associated with an increased volume of the parts of the brain responsible for mood and behavior.

To get out of a bad mood: A lack of selenium can cause bad moods. Individuals suffering from too little selenium have been shown to be more anxious, irritable, hostile and depressed than people with normal levels of selenium. Brazil nuts, salmon, and shitake mushrooms can instantaneously get you out of this funk.

When you want to feel happy: When we don't get enough exposure to sunlight, our mood and physical health may suffer. More specifically, serotonin levels, a hormone associated with elevating your mood rises when you're exposed to sunlight, leaving you to feel sad during the darker winter months. An amino acid, tryptophan helps raise serotonin levels in your body, causing you to feel upbeat once again. Eating foods that are high in tryptophan such as low-fat cottage cheese, nuts, and chicken will help boost your mood.

Get Moving: Studies show that anywhere from 30 minutes to an hour of exercise every day can have a positive impact on your mood. When we exercise our body releases endorphins that help us to feel happy. Exercise has also been shown to reduce stress, which can help alleviate feelings of depression brought on by the winter blues. Not to mention, frequent exercising can make your jeans fit a little better, and that's a mood booster in itself!

[Return to top] *Topic Area: Public Health & Healthcare*

FTC Site Still Down After Anonymous Hack; Anti-Piracy Fallout Spreads

By Kevin McCaney
GCN.com
January 25, 2012

The Federal Trade Commission's cybersecurity advice website remained offline Jan. 25, a day after it had been hacked by the group Anonymous in a continuing protest over proposed anti-piracy laws and recent anti-piracy arrests.

The OnGuardOnline.gov site, intended to give people cybersecurity advice, was hacked early Jan. 24, with the

home page replaced by the Anonymous logo, a rap song and a message threatening more attacks if anti-piracy legislation in Congress — which has stalled after a massive online protest Jan. 18 — were to pass.

FTC, which operates the site with several other agencies, took it offline after the hack.

The message left temporarily on OnGuardOnline referred to the Stop Online Piracy Act, The Protect Intellectual Property Act and the Anti-Counterfeiting Trade Agreement. If they pass, the message said, "we will wage a relentless war against the corporate Internet, destroying dozens upon dozens of government and company websites," The Next Web reported.

The message said Anonymous was "sitting on hundreds of rooted servers" and preparing to release information such as e-mail messages, passwords and bank account details.

SOPA and PIPA are bills introduced in the House and Senate, respectively, intended to combat piracy of intellectual property, especially by overseas criminal operations. But they both contain broad provisions requiring Internet service providers to block offending sites and search engines by rerouting traffic away from them that many Internet companies and users found objectionable.

On Jan. 18, thousands of websites, led by Reddit and Wikipedia, went dark in protest, posting messages urging people to oppose the bills, which began losing support from lawmakers shortly after.

The Anti-Counterfeiting Trade Agreement is a proposed international agreement for enforcing intellectual property rights that opponents claim would unduly restrict civil and digital rights.

A day after the SOPA protests, the piracy fight flared up on another front, after the FBI arrested leaders of the file-sharing site Megaupload and shut down the site.

Anonymous responded by attacking the websites of the Justice Department, FBI, White House and several entertainment industry companies.

DOJ said Megaupload, which claimed to have more than 150 million registered users and 50 million visitors a day, had made $175 million in illegal profits over about five years and caused a half-billion dollars in harm to copyright owners, particularly those in the recording industry.

The fallout from the arrests continued this week, with other file-sharing sites such as FileServe and FileSonic disabling their sharing services and saying users could download only content they had personally uploaded, ZDNet reported.

Meanwhile, Megaupload's American attorney defended the site's operations, telling ArsTechnica's Nate Anderson that it was no different than YouTube, in that it hosts shared content and shouldn't be held responsible for any content that has been pirated.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Ex-UCF Student Pleads Guilty To Federal Hacking Charge [FL]

By Amy Pavuk
Orlando Sentinel
January 25, 2012

A now former University of Central Florida student charged with hacking into a website used by the FBI recently pleaded guilty in federal court, records show.

Scott Matthew Arciszewski was arrested at his dorm on the UCF campus in July after investigators said he hacked into the Tampa Bay InfraGard site a month prior and uploaded three files.

Minutes after the unauthorized intrusion, federal prosecutors said, Arciszewski posted a thread on a hacker forum website that provided a link to InfraGard and instructions on how to exploit the site.

Soon after his posting, at least 15 hacking attempts were made to the website, seven of them being successful, court records said.

InfraGard is an FBI program designed to establish an alliance among academia, private industry and the federal agency, where members exchange information.

Court records also said that Arciszewski, using the Twitter name "voodooKobra," sent a message to the FBI's press office Twitter account stating that InfraGard "has one hell of an exploit."

Arciszewski was arrested on a federal hacking charge July 19, the same day agents across the country arrested more than a dozen others for their suspected roles in cyberattacks reportedly linked to the group Anonymous.

Documents filed by prosecutors said Arciszewski confessed to hacking into the InfraGard site.

Records show Arciszewski pleaded guilty in federal court in Tampa last week, and a judge accepted the plea and adjudicated him guilty Friday.

Arciszewski, no longer a UCF student, will be sentenced April 19 in Tampa.

He faces up to five years in federal prison, up to three years probation, and a fine up to $250,000.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Bizarre Skin Disease Morgellons Not Infectious, CDC Says

By Julie Steenhuysen
Reuters
January 25, 2012

After an exhaustive search, researchers at the Centers for Disease Control and Prevention have found no sign of an infectious agent, parasite or environmental exposure that could explain the mysterious skin condition known as Morgellons disease.

People with the condition complain of crawling, itching and stinging sensations and they often see tiny fibers or filaments that poke out of sores on their skin.

But the long-awaited government study, released on Wednesday in the journal PLoS One, found these fibers were mostly bits of cotton and nylon.

"We found no evidence that this condition is contagious, or that suggests the need for additional testing for an infectious disease as a potential cause," said Dr. Mark Eberhard, director of CDC's Division of Parasitic Diseases and Malaria, whose study appears in the journal PLoS One.

Eberhard said the study was not able to show the exact cause of the condition, but roughly half of the people in the study had illnesses, and most were psychiatric in nature.

Doctors have long suspected the condition was psychiatric rather than infectious.

Dr. Michael Cappello, a pediatric infectious disease expert at Yale University in New Haven Connecticut, has examined fibers taken from patients suffering from the condition.

"There really is not a controversy. The overwhelming number of physicians and investigators who have looked at this have come to the same conclusions," said Cappello, adding that it is commonly known by doctors as delusional parasitosis.

The strange condition was first described in 2002 by Mary Leitao of Pittsburgh who launched a website and advocacy campaign to identify a cause for the strange condition.

Prodded by an increasing number of reports and requests from lawmakers, the CDC embarked on a search for

the cause in 2006.

"It was clear these folks were actually suffering from something, many of them suffering a great deal. We felt compelled to address it," Eberhard said in a telephone interview.

The CDC team used medical records from the managed care company Kaiser Permanente in Northern California, where many of the people with reported symptoms lived, and studied 115 people with the condition.

"We tested for a wide range of infectious diseases," Eberhard said.

Many of the patients had full clinical exams and skin biopsies. Patients filled out questionnaires about whether they had been exposed to solvents or household chemicals, and patients got a comprehensive neuropsychiatric evaluation.

They found no signs that the condition was caused by an infection or environmental exposure. And studies of the fibers taken from sores in the skin showed they were largely composed of cotton or nylon, consistent with fibers found in clothing and carpeting.

Eberhard said people likely were scratching their skin and fibers in the environment stuck to their sores.

And the condition is rare, affecting only 4 out of 100,000 patients enrolled in the health plan.

Eberhard said ruling out an infectious cause should give doctors much more information about how to treat patients.

"We're really thrilled," Eberhard said. "Our sense is this should ultimately be very good for people suffering from this condition."

Cappello, who was not involved with the research, said he is glad the paper has finally been published.

"It is my hope that the CDC's findings can be accepted and that this issue, at least for the time being, can be put to rest," he said.

[Return to top] *Topic Area: Public Health & Healthcare*

Many Pediatric ICUs Have High Infection Rates

By Kevin McCarthy
Consumer Reports
January 26, 2012

Infections in pediatric intensive care units put children's lives at risk and occur all too often, according to a new investigation from the Consumer Reports Health Ratings Center. We found that pediatric ICUs often have higher infection rates than adult ICUs, and that some hospitals do much better than others at preventing infections.

Our investigation focused on a particularly dangerous type of infection—central-line bloodstream infections. We rated 92 pediatric ICUs in 31 states plus Washington, D.C., which publicly reported enough data for us to make statistically valid assessments of their rate of bloodstream infections. Those infections are fatal in as many as one in four cases.

We found that 26 of the 92 pediatric ICUs got low scores for infections, while only five pediatric ICUs earned our highest Rating, reporting zero infections.

Two pediatric ICUs—the University of Virginia Medical Center in Charlottesville and the Loyola University Medical Center in Maywood, Ill.—received our lowest Rating, which means they reported infection rates more than twice as high as the national average. Another 24 hospitals got our second-lowest Rating, with infection rates that were higher than the national average.

"Those hospitals have work to do, but at least they have taken the first step by making their results public," said

John Santa, M.D., director of the Consumer Reports Health Ratings Center. "Taking accountability for infections is reassuring. We're even more concerned about pediatric ICUs that choose to conceal their infection rates."

The five hospitals with zero infections are Children's Hospitals and Clinics of Minnesota in St. Paul; Medical University of South Carolina in Charleston; Robert Wood Johnson University Hospital in New Brunswick, N.J.; Tulane Medical Center in New Orleans; and University Medical Center in Las Vegas.

[Return to top] *Topic Area: Public Health & Healthcare*

Two Accused Of Trying To Smuggle Illegal Aliens To Ohio

Mohave Daily News
January 26, 2012

Mohave County Sheriff's deputies arrested two Maryland cousins near Littlefield on human smuggling charges, an MCSO spokeswoman said Wednesday.

Six suspected illegal immigrants were also taken into custody Sunday night after a traffic stop at Milepost 22 on Interstate 15.

At that time, spokeswoman Trish Carter said, deputies contacted eight occupants in van.

A Spanish-speaking officer from the Washington County (Utah) Sheriff's Office responded and assisted, she said.

With the assistance of Border Patrol, Carter said, six occupants were determined to be illegal immigrants. Border Patrol placed holds on them, she said.

During the course of the investigation, Carter said, authorities discovered that driver Henrry Leon-Zacarias, 29, and passenger Erwin Zacarias-Leon, 24, were transporting the illegal immigrants to Ohio.

Leon-Zacarias and Zacarias-Leon were arrested on felony charges of human smuggling and unlawful transport of aliens. They were transported to the Mesquite (Nev.) Detention Center. The illegal immigrants were transported to the Washington County Jail and later transferred into Border Patrol custody. The vehicle was towed from the scene.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Weekly Illicit Commercial Goods Report - 26 Jan 12

Download file

[Return to top] *Topic Area: Weekly DHS Illicit Commercial Goods Report*

Daily Infectious Diseases Report - 26 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Infectious Diseases Report*

Daily Human Trafficking Report - 26 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Human Trafficking and Smuggling Report*

Daily Terrorism Report - 26 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Terrorism Report*

Daily Cyber Report - 26 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS Cyber Report*

Daily Infrastructure Report - 26 Jan 12

Download file

[Return to top] *Topic Area: Daily DHS IP Report*

UNCLASSIFIED

From: OSINT Branch Mailbox
To: OSINT Branch Mailbox
Subject: DHS-OSE Homeland Security Central Digest - 2012-02-06
Date: Monday, February 06, 2012 7:04:05 AM
Attachments: DHS Daily Digest - 20120206.pdf

Classification: UNCLASSIFIED

(U) The DHS Homeland Security Central Digest for 06 February 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) Articles and resource documents come from open source information and are posted to the Homeland Security Central website on Intelink-U. For information on establishing an Intelink-U account, please visit http://ra.intelink.gov.

(U) The Homeland Security Central Digest contains full article text and may contain copyrighted material whose use has not been specifically authorized by the copyright owner. This information is available to DHS, in the interest of illuminating incidents and events that may have an impact on national security and critical infrastructure protection. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security

E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Digest
6 February 2012

Three Guilty Of Drug Trafficking [PA]

The jury deliberated for almost four hours yesterday before finding the three defendants in the Operation Drive Through trial guilty of operating a large cocaine and drug trafficking operation in Clearfield and Hyde. [HSEC-5.10]

Major Winter Storm Sweeping Across Colorado

A powerful winter storm swept across Colorado on Friday, forcing the state Department of Transportation to close portions of Interstate 70 and Interstate 25. The National Weather Service said snow was falling at 2 inches an hour on the Eastern Plains. [HSEC-2.1]

Human Trafficking Happening In Oklahoma City

It's something you'd picture in a third world country -- but it's happening right here in the metro -- human trafficking. Girls and boys used for sex while their pimps make a profit. [HSEC-3.10]

10 Kilos Of Cocaine Seized During Traffic Stop On NYS Thruway [NY]

Assistant U.S. Attorney John Duncan says, "10 kilos in a single seizure by the DEA represents one of the largest amounts of cocaine that's been recovered in a single arrest." As for its street value, Duncan says depending on how it's marketed, 10 kilos of cocaine can equal up to $10 million. [HSEC-5.10]

Mexican Man Convicted In Southern Arizona In Human Smuggling Case; To Be Sentenced In April

A Mexican man has been convicted in a human smuggling case in Arizona. Federal prosecutors say 26-year-old Berlain Galvez-Lopez was found guilty Wednesday in U.S. District Court in Tucson on three counts of smuggling immigrants for private financial gain. [HSEC-3.10]

Recall: Wegmans Cooked Eggs; Possible Listeria [NY, NJ]

Wegmans Food Markets is recalling hard-cooked eggs and prepared deli foods that contain hard-cooked eggs because of possible contamination with Listeria bacteria. [HSEC-6.1]

Norovirus Popping Up In MetroWest Hospitals [MA]

Local hospitals Thursday said there was an uptick this week in cases of a stomach bug called norovirus, a highly contagious illness that causes diarrhea, vomiting and stomach pain. [HSEC-6.1]

Anonymous Hacker Gives Details Of SLCPD Website Hack [UT]

The Salt Lake City Police Department website is still down today after being hacked on Tuesday night. Police are still trying to figure out exactly what was compromised. [HSEC-1.10]

Key Internet Operator VeriSign Hit By Hackers

VeriSign Inc, the company in charge of delivering people safely to more than half the world's websites, has been hacked repeatedly by outsiders who stole undisclosed information from the leading Internet infrastructure company. [HSEC-1.10]

Aurora Man Facing Terrorism-Related Charges Makes Court Appearance
An Aurora, Colo. man accused of trying to join a terrorist group overseas went before a judge in Denver federal court Thursday to be advised of the charges. [HSEC-8.10]

Cross-Border Methamphetamine Trade Booms And Mexico's 'War On Drugs'
The number of methamphetamine "super labs" seized by Mexican authorities has rocketed in the last five years but shipments of the drug across the border have also continued to grow, according to government statistics. [HSEC-3.10]

Terrorism No-Fly List Doubles
The Obama administration has more than doubled, to about 21,000 names, its secret list of suspected terrorists banned from flying to or within the United States, including about 500 Americans, The Associated Press has learned. [HSEC-8.9]

Full Text of all new articles....

Three Guilty Of Drug Trafficking [PA]

By Jeff Corcino
The Progress News
February 2, 2012

The jury deliberated for almost four hours yesterday before finding the three defendants in the Operation Drive Through trial guilty of operating a large cocaine and drug trafficking operation in Clearfield and Hyde.

Michael Styers, 55, of Mercer was the organization's ringleader, Charles Gearhart, 41, of Woodland was his second in command and Maharaji "Bean" Hemingway, 36, of Philadelphia was their primary supplier of cocaine, according to Dave Gorman, senior deputy attorney general.

However, Styers was found not guilty by the jury on all the charges related to the burglary of the Rite Aid pharmacy in Clearfield on Oct. 19, 2006, and the attempted burglary of the pharmacy on March 25, 2007. The jury found him guilty on all the drug possession and drug trafficking charges not related to the Rite Aid burglary.

Hemingway was also found not guilty of the false imprisonment charge of Autumn Kifer in 2007.

Gearhart was found guilty on all 19 charges against him.

In his closing statements Monday, Gorman said 19 witnesses testified at the trial that they had purchased cocaine from Styers at his South Fifth Street residence in Clearfield or had witnessed him sell drugs to other people.

Likewise, he said 16 people testified they had purchased or had witnessed someone purchase cocaine from Gearhart at his residence on Carr's Hill in Hyde where he often sold cocaine out of a window or at Styers's residence when Gearhart was unavailable.

He said nine witnesses testified they had purchased cocaine from Hemingway or had witnessed Hemingway sell cocaine to other people, including Styers and Gearhart.

However, Gorman admitted they had erred when they filed the false imprisonment charge for the imprisonment of Autumn Kifer during the summer of 2007. Several witnesses testified at the trial they believed the incident had occurred in the summer of 2006.

In addition, Hemingway was incarcerated in Philadelphia during the summer of 2007 and Judge Fredric Ammerman instructed the jury that Hemingway could only be convicted of the charge of false imprisonment if they

believed Kifer was falsely imprisoned in the summer of 2007.

Gorman said he was pleased with the jury's verdict.

"The jury sent a message to these defendants and the community that people who bring these poisons into Clearfield County will be stopped," Gorman said.

Gorman said this was a very large and important drug case and said the eight-day trial was the longest in his career with the Attorney General's Office.

He also praised the work of all law enforcement officials involved, especially lead investigator agent Dave Jordan of the Attorney General's Office.

"He poured his heart and soul into this case, and I applaud him for his work," Gorman said.

Styers' attorney Ben Vrobel expressed disappointment in the jury's verdict and said he plans to file an appeal.

"I find it difficult to accept that an individual can be convicted simply upon the words of thieves, addicts and cowards," Vrobel said.

Hemingway's attorney Lance Marshall had used the words "thieves, addicts and cowards" to question the credibility of the commonwealth's witnesses during his closing statement.

Gearhart's attorney Gary Knaresboro said he also plans to appeal the verdict.

"It's not over yet," Knaresboro said.

Marshall exited the courtroom before The Progress could reach him for comment, but during the trial, when he filed a motion for dismissal of the charges against his client, he informed Ammerman that he plans to appeal the verdict if his client is found guilty.

Ammerman thanked the jury for its diligence in serving through the lengthy trial where the members had to decide on 58 separate counts for three defendants.

Ammerman's jury instructions on the charges alone took more than two hours to complete before the jury could begin deliberating yesterday morning.

"For what just occurred over the past eight days in our little county, I suspect this is something you will remember for the rest of your lives," Ammerman told the jury.

This case was not only unique for its scope, but also for the length of time it took to get it to trial.

The charges were originally filed in 2008 and the trial had been scheduled for 2009 but was delayed due to legal procedures and appeals.

One delay was due to appeals regarding whether the Attorney General's Office had turned over the grand jury transcripts to defense attorneys in a timely manner and how the commonwealth should be sanctioned for not doing so.

Ammerman explained this delay at one point in the trial when the jury was out of the courtroom. According to Ammerman, he had ruled that the Attorney General's Office had failed to turn over the grand jury transcripts to the defense during the agreed upon time limit and therefore ruled the grand jury testimony would be excluded from trial.

However, the Attorney General's Office appealed his ruling and the Pennsylvania Court of Appeals ruled that although Ammerman was correct in his ruling, they believed the sanction to be too severe because it would essentially result in the dismissal of the case.

The defendants appealed the decision to the state Supreme Court, which denied their appeal on July 20, 2011.

The jury found Styers guilty on 18 drug possession and drug trafficking-related charges, and not guilty on all nine counts against him related to the Rite Aid break-ins.

The drug charges were separated into groups depending on date of occurrence.

The first group of charges was for offenses that occurred January 2005 through May 6, 2006. These charges are possession with the intent to deliver, cocaine; delivery of controlled substance, cocaine; possession with the intent to deliver heroine, delivery of a controlled substance, heroin; possession with the intent to deliver Oxycontin; delivery of a controlled substance, Oxycontin; possession with the intent to deliver, Fentanyl; delivery of a controlled substance; Fentanyl; criminal conspiracy with one or more persons with intent to deliver and delivery of a controlled substance, cocaine, heroin, Oxycontin and Fentanyl; dealing in the proceeds of unlawful activities.

The second group was for offenses that occurred between Sept. 28, 2006 and June 14, 2007. They are possession with intent to deliver cocaine; delivery of a controlled substance, cocaine; possession with intent to deliver Oxycontin; delivery of controlled substance, Oxycontin dealing in the proceeds of unlawful activities; criminal use of a communication facility.

He was also found guilty of corrupt organizations; corrupt organizations: conspiracy with other persons for offenses between January 2005 through June 14, 2007.

He was found not guilty on the charges relating to the Rite Aid burglary on Oct. 19, 2006: burglary; criminal conspiracy with one or more persons to commit possession with intent to deliver and delivery of controlled substances; theft by unlawful taking; receiving stolen property; criminal conspiracy to commit burglary; possession with intent to deliver controlled substances from Rite Aid burglary; delivery of controlled substances from Rite Aid burglary.

He was also found not guilty on the following charges relating to the attempted burglary of Rite Aid on March 25, 2007: criminal attempt to commit burglary and criminal trespass

Gearhart was found guilty on all 19 counts against him. They are 12 counts of delivery of a controlled substance, cocaine January 2005 to June of 2007 with one count each for delivery to the following people: Danielle Gearhart, Jodi Wilkinson, Rick Wilkinson, Joseph Hunter, Brandon Kifer, Michael S. Gearhart, Denny Daub, Autumn Kifer, Greg Ordrosky, Darla Daub, Aszure Luzier and Robert Charles.

He was also found guilty of two counts of possession with intent to deliver; criminal conspiracy with one or more persons to commit possession with the intent to deliver and delivery of a controlled substance; criminal use of a communication facility; dealing in the proceeds of unlawful activity, corrupt organizations; corrupt organizations, conspiracy with other persons. All Gearhart's charges were for offenses between January 2005 and June 2007.

Hemingway was found guilty on 11 of the 12 charges against him.

They are six counts of delivery of a controlled substance, one count each for delivery to the following individuals, Styers, Gearhart, Joseph Hunter, Richard Smeal, and Kristen Wilsoncroft; criminal use of a communication facility; dealing in the proceeds of unlawful activities; corrupt organizations and corrupt organizations, conspiracy with other persons.

All charges against Hemingway were for offenses that occurred between January 2005 and June 2007.

[Return to top] *Topic Area: Illegal Drug Trafficking*

Major Winter Storm Sweeping Across Colorado

By Steven K. Paulson
ABC News
February 3, 2012

A powerful winter storm swept across Colorado on Friday, forcing the state Department of Transportation to close

portions of Interstate 70 and Interstate 25. The National Weather Service said snow was falling at 2 inches an hour on the Eastern Plains.

Transportation spokeswoman Becky Navarro said Friday eastbound I-70 was closed from Aurora to Limon and a ramp has been closed on Interstate 25 in Denver because of numerous accidents.

"There are a lot of areas on the Front Range where there is very poor visibility," she said.

The largest snow total Friday morning was 18 inches in Pinecliff west of Denver.

Jim Kalina of the National Weather Service said another foot of snow was expected in some areas along the Front Range before the storm moves out on Saturday. A blizzard warning was issued through Saturday for northeastern Colorado where sustained winds of up to 30 mph could bring visibility to zero and make travel all but impossible.

Cities in the Front Range urban corridor from Colorado Springs in the south to Fort Collins and Greeley in the north were under a winter storm warning.

The storm warnings prompted shoppers to stock up on food and liquor, while Colorado lawmakers canceled legislative work on Friday.

Stores in Denver reported brisk business Thursday night.

"The cheese wall is hammered, bread's kind of hammered, milk's kind of low," said Aaron McFadden, a manager at a King Soopers store.

Ted Vaca at Argonaut Liquor said customers were snapping up all kinds of drink.

"It was more like a Friday than a Thursday," he said.

The storm forced the cancellation of more than 150 arriving and departing flights at the Denver airport that had been scheduled through Friday night.

A Learjet ran off a runway at the Pueblo airport as the storm moved in, but investigators hadn't determined if the weather was a factor. None of the 10 people aboard was injured, the Federal Aviation Administration said.

Many school districts announced they would be closed on Friday, including the two largest, in Jefferson County and Denver.

The storm could break into the top 10 list of the heaviest snowstorms in Denver history. The city's 10th biggest dumped 22.1 inches in 1912, NWS meteorologist Chad Gimmestad said.

Denver's record is 45.7 inches from a five-day wallop in 1913.

Parts of Wyoming, Nebraska, Iowa and Kansas were also predicted to be hit by the storm.

[Return to top] *Topic Area: Winter Storms & Cold Snaps*

Human Trafficking Happening In Oklahoma City

By Amanda Taylor
News 9
February 2, 2012

It's something you'd picture in a third world country -- but it's happening right here in the metro -- human trafficking.

Girls and boys used for sex while their pimps make a profit.

The numbers are staggering. More and more metro children sold into the world of modern day slavery and it

doesn't always start the way we might think.

Last Fall we introduced you to Samantha, a 38 year old metro woman who was trafficked as a teenager. Her story is frightening for any parents to hear.

"I was taken and sold against what I wanted. It wasn't my choice, I wasn't given a choice. Prostituted out, not a prostitute, but prostituted out and that's a big difference" she says.

Mark Elam with OATH - Oklahomans Against Trafficking Humans says the numbers are staggering and something as simple as a lack of support at home can cause our children to be pointed down the wrong path.

"The majority is a relationship danger issue. They trust this person. They've made promises. They go with them to get out of a difficult situation. They don't feel valued. They're looking for attention or care."

It's a growing problem that hits close to home. Samantha says it's happening right in our own backyards.

"It needs to be known it happens in Oklahoma. It happens at 10th & McKinley, it happens at McKinley Park, at the McDonald's off I-40, it happens."

And just knowing the wrong people can be enough.

Last October Bethany police found the dismembered body of 19-year-old Carina Saunders behind a Homeland grocery store. Police later arrested Jimmy Massey and charged him in connection with Saunders' murder. Police say the motive is trafficking.

Elam says it's a warning sign for metro parents.

"If one girl starts acting out, they'll beat her as an example in front of the other girls. It's not often they'll murder her because their intention is to make profit. They want these girls to make them money so killing them isn't a profitable situation."

He says there are simple ways to help protect our children.

"It's about being a part of their life. Not telling them what to do or not to do, warning them about dangers. I think they know about the dangers, but they're in love or think that wouldn't happen to them, so it's really about being a part of their life and caring enough to spend time with them."

OATH hopes the Saunders tragedy gets the attention of parents who might be worried about their kids and cause them to jump in and help.

Samantha's message for victims is simple. "It's not your fault, it's not you."

Samantha adds while it can seem impossible at the time, victims need to speak up and seek help.

That help can be a phone call away.

OATH's hotline is 1-800-955-0128.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

---

10 Kilos Of Cocaine Seized During Traffic Stop On NYS Thruway [NY]

9WSYR.com
February 2, 2012

State police have arrested three people after a search of their vehicle led to the discovery of 10 kilos of cocaine.

Texas residents Ruby Irene Maxwell, 30, Mary Ann Selgado, 41, and Matthew Octavious Sandoval, 33 were observed by DEA agents Wednesday night as being associated with a mid-level member of the violent Mexican

drug cartel Los Zetas.

DEA agents notified State Police, who in turn stopped the vehicle on the New York State Thruway near Exit 37 in the Town of Salina.

A drug canine was called in to assist and alerted police to the presence of cocaine. A search of the vehicle led to 10 kilograms of cocaine hidden in secret compartments throughout the vehicle.

Assistant U.S. Attorney John Duncan says, "10 kilos in a single seizure by the DEA represents one of the largest amounts of cocaine that's been recovered in a single arrest."

As for its street value, Duncan says depending on how it's marketed, 10 kilos of cocaine can equal up to $10 million.

Each of the suspects has been charged with conspiracy to possess with intent to distribute

If convicted, the offense carries a minimum sentence of ten years incarceration and a maximum life sentence, as well as a fine of $10 million.

Maxwell, Selgado and Sandoval are being held pending a detention hearing set for Friday.

[Return to top] *Topic Area: Illegal Drug Trafficking*

Mexican Man Convicted In Southern Arizona In Human Smuggling Case; To Be Sentenced In April

The Associated Press
February 3, 2012

A Mexican man has been convicted in a human smuggling case in Arizona.

Federal prosecutors say 26-year-old Berlain Galvez-Lopez was found guilty Wednesday in U.S. District Court in Tucson on three counts of smuggling immigrants for private financial gain. He's scheduled to be sentenced on April 12.

U.S. Border Patrol agents in the Casa Grande area discovered several footprints after responding to detection technology while patrolling in the west desert last November.

Agents tracked the footprints for several miles before encountering a group of individuals who had entered Arizona illegally. All subjects were apprehended and transported to the Casa Grande Station for processing.

During processing, agents identified Galvez-Lopez as the foot guide or "coyote." A records check also revealed Galvez-Lopez had two prior deportations for being in the country illegally.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Recall: Wegmans Cooked Eggs; Possible Listeria [NY, NJ]

The Associated Press / The Wall Street Journal
February 2, 2012

Wegmans Food Markets is recalling hard-cooked eggs and prepared deli foods that contain hard-cooked eggs because of possible contamination with Listeria bacteria.

The products were sold between Jan. 23 and Feb. 1 at Wegmans stores in Rochester, Buffalo, Syracuse, Canandaigua, Newark, Geneva, Corning, Elmira, Geneseo, and Hornell. It's the result of a recall by Minnesota-based Michael Foods, which produces the cooked eggs at its Wakefield, Neb. facility.

Listeria can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with

weakened immune systems. Healthy people may suffer only short-term symptoms such as fever, headache, nausea and diarrhea.

There have been no reports of illness.

The products include deviled eggs, egg salad, and several deli salads with eggs.

[Return to top] *Topic Area: Public Health & Healthcare*

Norovirus Popping Up In MetroWest Hospitals [MA]

By Laura Krantz
MilfordDailyNews.com
February 3, 2012

Local hospitals Thursday said there was an uptick this week in cases of a stomach bug called norovirus, a highly contagious illness that causes diarrhea, vomiting and stomach pain.

"Now we're seeing two to three people come through the (emergency department) a day," said Melissa Hodgson, spokesperson for Marlborough Hospital.

She said they don't usually see any.

According to the Centers for Disease Control, a norovirus infection causes acute gastroenteritis, whose symptoms also include dehydration and stomach pain.

Michael Gottlieb, chief medical officer at MetroWest Medical Center, said 10 to 20 percent of cases in the emergency department over the past few weeks have been stomach bugs.

"There is a lot of pervasive gastrointestinal illness in the community and I have no doubt that a lot of it is norovirus," Gottlieb said.

However, he said most caregivers don't test for norovirus, but instead treat the dehydration, diarrhea or vomiting.

"We would treat the symptoms," said registered nurse Donna O'Connor, director of case management and infection control at Marlborough Hospital.

She recommended people who have norovirus symptoms drink water and stay home and away from others for 48 to 72 hours.

They should wash their hands frequently and wash surfaces, including counters and doorknobs, she said.

Milford Regional Medical Center spokesperson Terri McDonald said they had more cases this week among both patients and hospital staff.

The state's Department of Public Health spokesperson Jennifer Manley said that isn't abnormal.

"It is an increase that we expect this time of year," she said.

Manley said outbreaks are most common in dormitories, nursing homes and assisted living facilities.

[Return to top] *Topic Area: Public Health & Healthcare*

Anonymous Hacker Gives Details Of SLCPD Website Hack [UT]

By Shara Park and Randall Jeppesen
KSL.com
February 2, 2012

The Salt Lake City Police Department website is still down today after being hacked on Tuesday night. Police are still trying to figure out exactly what was compromised.

The hacking group calling themselves Anonymous said it got all kinds of information from the SLCPD, including phone numbers, addresses, email addresses and potentially more.

A person claiming to be a part of the group has been interacting with Salt Lake media through Twitter and said that the hack gave Anonymous information on drug operations, sales suppliers, license plate numbers and more.

Salt Lake Police said this person on Twitter is likely linked somehow to the group that got into their website.

"Somehow they are affiliated they're in the know," said Sgt. Shawn Josephson of SLCPD. "As far as what their involvement is, we're not sure at this point, but we are definitely keeping those details in mind and following those same things that you are receiving."

Officials said all the information was from what people submitted through tip forms on the website.

Other compromised information includes names and numbers of people who wanted to know more about job openings at the police department, but this did not include full resumes.

Lake police said the hack doesn't prevent them in any way from doing their job, but it does harm their relationship with the public through online tips. SLCPD won't put the website back up until they can make sure it is secure.

Several local journalists chatted with a supposed member of the Anonymous involved in the hack over Twitter, including KSL's Shara Park. While it is not yet possible to say whether the person's claims are true, the hacker provided files that were stolen from Salt Lake Police - one of which is an unpublished complaint submitted by a citizen.

In a private chat room under the name "Kahuna," the hacker explained why he stole thousands of documents from the Salt Lake City Police Department's website.

"Daily we watch cops beat people, arrest them without cause, and this is a message that we are watching and that we see this as unlawful," he wrote. "Kahuna" referred to SB107, a bill that would criminalize the possession of any instrument, tool or device used to make with the intent of defacing another's property. He wrote that if the bill passes, he will target the "foot soldiers" that enforce it, and said he would release information about the police officers involved with this, knowing that it would put them at risk.

The bill failed in the senate Thursday.

Essentially, "Kahuna" was able to hack their site and through that, gained admin logins and passwords. From there he was able to access an internal server and get more private information from the department.

"Kahuna" said he is the only person with a copy of all the stolen information and will not release it.

"Innocent civilians reporting crimes are not my target," he wrote.

His message for those citizens who feel their information is in danger he writes, "Nothing in this is a target to you, we are not out to cause you any harm nor would we ever do so..."

Nevertheless, to the police he wrote, "If this bill continues and passes and causes a single arrest of intent, this won't be the only time they hear from us, and they better expect us."

The hacker says Salt Lake City Police are underplaying just how much sensitive and compromising information he was able to get.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Key Internet Operator VeriSign Hit By Hackers

By Joseph Menn
Reuters
February 2, 2012

VeriSign Inc, the company in charge of delivering people safely to more than half the world's websites, has been hacked repeatedly by outsiders who stole undisclosed information from the leading Internet infrastructure company.

The previously unreported breaches occurred in 2010 at the Reston, Virginia-based company, which is ultimately responsible for the integrity of Web addresses ending in .com, .net and .gov.

VeriSign said its executives "do not believe these attacks breached the servers that support our Domain Name System network," which ensures people land at the right numeric Internet Protocol address when they type in a name such as Google.com, but it did not rule anything out.

VeriSign's domain-name system processes as many as 50 billion queries daily. Pilfered information from it could let hackers direct people to faked sites and intercept email from federal employees or corporate executives, though classified government data moves through more secure channels.

"Oh my God," said Stewart Baker, former assistant secretary of the Department of Homeland Security and before that the top lawyer at the National Security Agency. "That could allow people to imitate almost any company on the Net."

The VeriSign attacks were revealed in a quarterly U.S. Securities and Exchange Commission filing in October that followed new guidelines on reporting security breaches to investors. It was the most striking disclosure to emerge in a review by Reuters of more than 2,000 documents mentioning breach risks since the SEC guidance was published.

Even if the name system is safe, VeriSign offers a number of other services where security is paramount. The company defends customers' websites from attacks and manages their traffic, and it researches international cybercrime groups.

VeriSign would possess sensitive information on customers, and its registry services that dispense website addresses would also be a natural target.

Ken Silva, who was VeriSign's chief technology officer for three years until November 2010, said he had not learned of the intrusion until contacted by Reuters. Given the time elapsed since the attack and the vague language in the SEC filing, he said VeriSign "probably can't draw an accurate assessment" of the damage.

Baker said VeriSign's description will lead people to "assume that it was a nation-state attack that is persistent, very difficult to eradicate and very difficult to put your hands around, so you can't tell where they went undetected."

VeriSign declined multiple interview requests, and senior employees said privately that they had not been given any more details than were in the filing. One said it was impossible to tell if the breach was the result of a concerted effort by a national power, though that was a possibility. "It's an ugly, slim sliver of facts. It's not enough," he said.

The 10-Q said that security staff responded to the attack soon afterward but failed to alert top management until September 2011. It says nothing about a continuing investigation, and the Department of Homeland Security did not respond to questions about an inquiry or recommendations for VeriSign customers.

Until August 2010, VeriSign was one of the largest providers of Secure Sockets Layer certificates, which Web browsers look for when connecting users to sites that begin "https," including most financial sites and some email and other communications portals.

If the SSL process were corrupted, "you could create a Bank of America certificate or Google certificate that is trusted by every browser in the world," said prominent security consultant Dmitri Alperovich, president of Asymmetric Cyber Operations.

VeriSign sold its certificate business in the summer of 2010 to Symantec Corp, which has kept the VeriSign brand name on those products.

Symantec spokeswoman Nicole Kenyon said "there is no indication that the 2010 corporate network security breach mentioned by VeriSign Inc was related to the acquired SSL product production systems."

Some smaller issuers of such validation certificates have been compromised in the past, and false certificates have been used to spread the most sophisticated malicious software yet detected, including Stuxnet, which attacked the Iranian nuclear program.

In written Senate testimony on Tuesday, U.S. Director of National Intelligence James Clapper called the known certificate breaches of 2011 "a threat to one of the most fundamental technologies used to secure online communications and sensitive transactions, such as online banking." Others have said SSL as a whole is no longer trustworthy and effective.

In a section of its filing devoted to risk factors, VeriSign said it was a frequent subject of "the most sophisticated form of attacks," including some that are "virtually impossible to anticipate and defend against."

Security experts said the breach reminded them of last year's attack on RSA, an authentication company owned by storage maker EMC Corp. RSA's SecurID tokens authorize remote access and have been in wide use by government agencies and military contractors including Lockheed Martin Corp, which said it was probed on the heels of the RSA breach.

"This breach, along with the RSA breach, puts the authentication mechanisms that are currently being used by businesses at risk," said Melissa Hathaway, a former intelligence official who led U.S. President Barack Obama's cybersecurity policy review and later pushed for the SEC guidance. "There appears to be a structured process of hunting those who provide authentication services."

Even if VeriSign's certificates were not compromised, a significant breach "means that prevention is futile," Alperovich said. He said he hoped new legislation on cybersecurity, expected to reach the Senate floor this month, would call for more disclosures and bring more aid to companies under attack.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Aurora Man Facing Terrorism-Related Charges Makes Court Appearance

Fox 31 Denver
February 2, 2012

An Aurora, Colo. man accused of trying to join a terrorist group overseas went before a judge in Denver federal court Thursday to be advised of the charges.

Jamshid Muhtorov, 35, is charged with one count of providing material support of a designated foreign terrorist organization.
He was arrested at Chicago's O'Hare airport in January while en-route to Istanbul, Turley, federal prosecutors said.

During Thursday's advisement, Magistrate Judge Kathleen M. Tafoya asked Muhtorov if he wanted a court-appointed attorney, but he refused to answer. Instead, he asked to speak with his wife.

The judge said he could not speak with his wife until he had legal counsel.

According to the U.S. Attorney's Office, Muhtorov, who also goes by the names Abumumin Turkistony and Abu Mumin, had ongoing communications with leaders of the Islamic Jihad Union (IJU), an extremist group that splintered from the Islamic Movement of Uzbekistan in the early 2000s.

The IJU, according to the Department of Justice, has been linked to numerous attacks in Uzbekistan and against coalition forces in Afghanistan dating back to 2004.

Fox 31 Denver

[Return to top] *Topic Area: Terrorism Support & Financing*

Cross-Border Methamphetamine Trade Booms And Mexico's 'War On Drugs'

By F. Brinley Bruton
MSNBC
February 3, 2012

The number of methamphetamine "super labs" seized by Mexican authorities has rocketed in the last five years but shipments of the drug across the border have also continued to grow, according to government statistics.

The increase highlights how Mexico's cartels have diversified beyond their traditional focus of exporting cocaine, heroin and marijuana by transforming their operations to also make methamphetamines on an industrial scale.

The U.S. Drug Enforcement Administration (DEA) has noted "a sustained upward trend in Mexican methamphetamine availability in U.S. markets." Research by the U.S. government also shows that methamphetamine prices are falling and that the purity level of seizures is rising.

According to information from Mexico's Secretariat of National Defense, 22 methamphetamine labs were seized in 2007. That number increased to 206 in 2011.

The vast majority of these were classed as super labs – in contrast to smaller operations that characterize much of the production in the United States, a secretariat official confirmed to msnbc.com. The official asked for anonymity for security reasons.

"Methamphetamine seizure rates inside the United States and along the U.S.-Mexico border have increased markedly since 2007," according to a U.S. Department of Justice report.

'In the business of making money'

U.S. Drug Enforcement Administration (DEA) officials said they could not comment specifically on statistics released by the Mexican government, but acknowledge that the cartels have adapted and changed since President Felipe Calderon declared his war on drugs in December 2006.

"There has been an evolution," Special Agent Gary Boggs of the DEA's Office of Diversion Control told msnbc.com. "All of these drug trafficking groups, they are not in the business of drugs, they are in the business of making money. So regardless of what the drug is, if there is a market for it they are going to try ways of making money out of it."

Methamphetamine, a white, odorless and bitter crystalline powder, dissolves in water or alcohol and can be taken orally, snorted, injected or smoked. Known as meth, chalk, go-fast, zip, ice and crystal, among other names, it can be very addictive and lead to dramatic weight loss, dental problems, paranoia, hallucinations and extreme violence.

The methamphetamine trade is only part of the drug problem confronting Mexico – the country's cartels also produce or traffic large amounts of cocaine, heroin and marijuana, among other narcotics. Since Calderon's war on drugs began, more than 47,500 people have been killed, according to the country's attorney general's office. The worsening violence and continued flow of drugs has caused many to question whether Mexico's militarized approach is the right way to stamp out the cartels.

While most of the bloodshed in the war on drugs has been south of the border, the problem has had a direct impact on Americans. Mexico is the primary source of methamphetamines consumed in the U.S., according to the Department of Justice's National Drug Threat Assessment 2011.

"Methamphetamine production in Mexico is robust and stable, as evidenced by recent law enforcement reporting, laboratory seizure data, an increasing flow from Mexico, and a sustained upward trend in Mexican methamphetamine availability in U.S. markets," according to the study, which bases its conclusions on data running through September 2010. "Law enforcement and intelligence reporting, as well as seizure, price, and purity data, indicate that the availability of methamphetamine in general is increasing in every region of the (United States)."

According to the Department of Justice report, from July 2007 through September 2010, the price per pure gram of methamphetamine decreased 60.9 percent, from $270.10 to $105.49. Purity increased 114.1 percent, from 39 percent to 83 percent.

Booming business

After declining sharply in 2007, methamphetamine seizures along the Mexico-U.S. border have increased every year.

The dramatic growth in operations targeting Mexican methamphetamine super labs from 2007 and 2011 is likely the result of the huge increase in military involvement during Calderon's war on drugs, said Octavio Rodriguez, coordinator of the Justice in Mexico Project at the University of San Diego's Trans-Border Institute.

This jump in decommissions cannot be taken alone, however – falling prices also suggest that the trade in methamphetamines remains a booming business despite the enormous military deployment.

"My impression is that this data shows a much greater effectiveness on the part of the army," Rodriguez told msnbc.com. "But what these numbers imply to me is that if lab seizures are growing and the price is falling is that the production is so high that it is not causing a serious impact. In other words, if seizures are not having a real effect on prices and the price continues to fall it means that the seizures aren't even affecting the level of production."

Since 2007, Mexican spending on security, which includes the army, navy, federal police and attorney general's office, has almost doubled to reach more than $46 billion.

The United States, the world's largest consumer of illegal drugs, had spent around $1.4 billion since 2008 on the struggle against the cartels in Mexico and Central America as part of the so-called Merida Initiative. Meanwhile, U.S. border patrols costing the United States $3 billion per year have helped make the nearly 2,000-mile-long boundary as fortified as it has been in 160 years, according to a report by the Council of Foreign Relations.

But despite the billions spent and tens of thousands of lives lost, the organization thought to be controlling much of the methamphetamine trade as well as heroin and marijuana, the Sinaloa cartel, remains staggeringly powerful. In January, Joaquin "El Chapo" Guzman, at the helm of the group believed to control the methamphetamine trade and the drug's key ingredients, earned the title of "world's most powerful drug trafficker" from the U.S. Department of Treasury.

Guzman has also appeared on Forbes' World's Most Powerful People list since 2009, and is thought to be the world's richest drug dealer, according to the magazine.

Key chemicals

Officials say key to stamping out the methamphetamine trade is interrupting the flow of chemicals needed to

manufacture it, known as precursors.

China and India are the main countries involved in the trafficking of key precursor chemicals to Mexico, the DEA's Boggs said

"We've … taken steps to work with our international partners to curb international chemical smuggling," he added.

Despite efforts by officials on both sides of the border, the trade in methamphetamines and precursors is likely spreading south. According to The Associated Press, 1,600 tons of precursors were seized in Guatemala in 2011, up from 400 seized there in 2010.

In December alone, 675 tons of precursors destined for Guatemala were seized in Mexico. Most of it came from Shanghai, China, the AP reported. At $100 per gram for the finished product, that would end up producing hundreds of billions of dollars-worth of drugs.

A soldier guards boilers at an outdoor clandestine methamphetamine laboratory discovered in Chiquilistlan, Mexico, on December 7. (Alejandro Acosta | Reuters)

[Return to top] *Topic Area: Illegal Drug Trafficking*

Terrorism No-Fly List Doubles

Newsday
February 2, 2012

The Obama administration has more than doubled, to about 21,000 names, its secret list of suspected terrorists banned from flying to or within the United States, including about 500 Americans, The Associated Press has learned. The government lowered the bar for the list, even as it says it is closer than ever to defeating al-Qaida.

The size of the list has jumped from about 10,000 in the past year, according to government figures provided to the AP. The surge comes as the government says it is close to defeating al-Qaida, after killing many of its senior members. But senior officials said the threat does not stop there.

"As long as we sustain the pressure on it, we judge that core al-Qaida will be of largely symbolic importance to the global jihadist movement," Director of National Intelligence James Clapper told Congress yesterday. "But regional affiliates and, to a lesser extent, small cells and individuals will drive the global jihad agenda."

"Both U.S. intelligence and law enforcement communities and foreign services continue to identify people who want to cause us harm, particularly in the U.S. and particularly as it relates to aviation," Transportation Security Administrator John Pistole said.

The flood of new names began after the failed Dec. 25, 2009, attempted bombing of a Detroit-bound jetliner. The government does not disclose who is on the list or why anyone is on it.

[Return to top] *Topic Area: Counter Terrorism*

Daily Infectious Diseases Report - 03 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Infectious Diseases Report*

Daily Human Trafficking Report - 03 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Human Trafficking and Smuggling Report*

Daily Terrorism Report - 03 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Terrorism Report*

Daily Cyber Report - 03 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Cyber Report*

Daily Infrastructure Report - 03 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS IP Report*

UNCLASSIFIED

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Homeland Security Central Digest - 2012-02-10
Date:	Friday, February 10, 2012 7:12:23 AM
Attachments:	DHS Daily Digest - 20120210.pdf

Classification: UNCLASSIFIED

(U) The DHS Homeland Security Central Digest for 10 February 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) Articles and resource documents come from open source information and are posted to the Homeland Security Central website on Intelink-U. For information on establishing an Intelink-U account, please visit http://ra.intelink.gov.

(U) The Homeland Security Central Digest contains full article text and may contain copyrighted material whose use has not been specifically authorized by the copyright owner. This information is available to DHS, in the interest of illuminating incidents and events that may have an impact on national security and critical infrastructure protection. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,

- - - - - -

Open Source Content Management
Department of Homeland Security

E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Digest
10 February 2012

B.C. Men Face Extradition In Cross-Border Drug Ring

Two B.C. men face extradition to the U.S. after being linked to a busted cross-border, drug-smuggling operation. Duc Thi Nguyen, 48, faces charges of conspiracy to distribute controlled substances and the distribution of cocaine and methamphetamine. [HSEC-5.10]

22 Facing Federal Prison For Gun Trafficking [TX]

A total of 22 San Antonio residents are headed to federal prison in connection with an illegal gun trafficking operation believed to be tied to Mexican drug dealers. [HSEC-10.10]

Human Trafficking Spotlight Focused On South County [FL]

In a Pinellas County beach community, young women were held captive in a large waterfront house without clothes, money or identification, forced to work in local commercial sex trade joints strictly for the pleasure and profit of others. [HSEC-3.10]

Report: Super Bowl Fans Possibly Exposed To Measles In Indianapolis

The cost for fans to attend the Super Bowl is sky-high, but possible exposure to measles could make the price much higher than anyone expected. [HSEC-6.1]

Chicken Salad Sandwiches Another Egg-Related Recall

Grand Strand Sandwich Company of Longs, SC is recalling some of its chicken salad sandwiches from convenience stores in the Southwest after its distributor recalled the chicken salad used to make them. [HSEC-6.2]

Alleged JPL Computer Hacker Indicted [CA]

A Romanian man who allegedly hacked into Jet Propulsion Laboratory computers and interfered with NASA satellite research was indicted this week by a federal grand jury. [HSEC-1.10]

Wyola Man Admits Eagle Trafficking [MT]

Wyola resident Ernie Lemuel Stewart admitted Wednesday that he baited eagles, killed them and sold their carcasses for thousands of dollars. [HSEC-4.10]

Hacker Group 'Anonymous' Tried To Extort Payment From Symantec

Symantec Corp. (SYMC) is bracing for the release of more purloined source code in coming weeks following the disclosure that an individual claiming to be part of "Anonymous" attempted to extort payment from the company in exchange for not making the code public. [HSEC-1.10]

Jacksonville Group Rescues Human Trafficking Victims [FL]

On the streets of Jacksonville lurks a dangerous network of human trafficking. Many are runaway teens, some under the age of 14. Others have been shipped to the U.S. All are being sold for sex. [HSEC-3.10]

Judge Allows Secret Surveillance Evidence In July Trial Of Iraqi On Terrorism Charges In Ky.
Secret documents suggest an Iraqi man facing charges of trying to funnel weapons and cash to al-Qaida operatives in his home country was "an agent of a foreign power," and his lawyers may not see or suppress those documents, a judge ruled Wednesday. [HSEC-8.10]

Full Text of all new articles....

B.C. Men Face Extradition In Cross-Border Drug Ring

By Mike Raptis
The Province
February 9, 2012

Two B.C. men face extradition to the U.S. after being linked to a busted cross-border, drug-smuggling operation.

Duc Thi Nguyen, 48, faces charges of conspiracy to distribute controlled substances and the distribution of cocaine and methamphetamine.

Nguyen Quach, age unknown, faces charges of conspiracy to distribute controlled substances and the distribution of cocaine.

The drug-smuggling ring - a multi-million-dollar operation as far-reaching as Mexico, B.C. and across the U.S. - was officially brought down in U.S. District Court in Seattle on Wednesday when its leader, Drew Yim, 38, of Burien, Wash. pleaded guilty to conspiracy and money-laundering charges.

Yim faces a mandatory minimum 10 years in prison and up to life in prison when sentenced in May.

He and 13 others were arrested in May 2011. Four additional defendants are fugitives.

Of the defendants in custody, all but two have pleaded guilty.

The investigation involved law enforcement in both the U.S. and Canada.

In his plea agreement, Yim admitted to leading a criminal enterprise with dozens of conspirators. He used as many as 18 cellphones and directed massive shipments of cocaine and meth from California into Washington and into B.C.

In June 2010, March 2011 and May 2011, more than 55 kilograms of cocaine were transported into B.C.

From B.C., Yim directed the importation and distribution of ecstasy and B.C. Bud into Washington and the rest of the U.S.

Over five months in 2010, Yim arranged for more than 700 pounds of B.C. Bud to be transported into the U.S.

Yim is also forfeiting millions of dollars in cash, possessions and real estate.

Of the two Canadians involved, Duc Thi Nguyen was found guilty in Vancouver of possession of property obtained by crime in 2005 but was never jailed.

He also faced a charge of conspiracy to commit an indictable offence in 2005 but a trial date was cancelled.

Duc Thi Nguyen was also found guilty of fisheries violations in the waters off Courtenay in 2001, along with two others.

Nguyen Quach's only offence is a speeding violation in Vancouver in October 2000.

[Return to top] *Topic Area: Illegal Drug Trafficking*

22 Facing Federal Prison For Gun Trafficking [TX]

By Katrina Webber
KSAT
February 8, 2012

A total of 22 San Antonio residents are headed to federal prison in connection with an illegal gun trafficking operation believed to be tied to Mexican drug dealers.

Nine people have been sentenced so far to prison terms ranging from one to 14 years.

Two of them learned their fate Tuesday in U. S. District Court in Del Rio. Keith Edwards, 23, was sentenced to 87 months in prison, while Ricky Gonzales, 22, has been ordered to serve out a 42-month sentence.

Other defendants are scheduled to be sentenced during this month, and in March and April.

Edwards and Gonzales are among 22 people who pleaded guilty to charges related to what the U. S. Attorney's Office calls a "straw purchasing" operation.

It involves people who have no criminal record purchasing weapons from legitimate gun dealers, then turning them over to others. The "straw purchasers" usually are paid a few hundred dollars for their involvement, investigators said.

"These weapons were destined for Mexico, no doubt. They were destined for organized crime, the cartels that are operating in Mexico," said Jerry Robinette, special agent in charge with U.S. Immigration and Customs Enforcement (ICE).

ICE was one of several federal agencies that took part in the investigation. It began with a tip federal agents received in May 2010.

According to a news release, the defendants include two men who are believed to be the ring leaders of the operation, Marino Castro, Jr., 27, and Edward Levar Davis, 33.

Investigators said Castro recruited his own mother and aunt for the operation, as well as eight housewives and more than a half dozen people in their 20s.

U. S. Attorney Robert Pitman, Western District of Texas, said the case should serve as a warning to others who might be considering taking part in this type of behavior.

"Even if that role is being paid a couple of hundred dollars for buying a firearm and passing it off to a middle man, it will net them a prison sentence for up to 10 years," Pitman said.

[Return to top] *Topic Area: Weapons Trafficking*

Human Trafficking Spotlight Focused On South County [FL]

By Melody Jameson
Observer News
February 9, 2012

In a Pinellas County beach community, young women were held captive in a large waterfront house without clothes, money or identification, forced to work in local commercial sex trade joints strictly for the pleasure and profit of others.

In Boca Raton, more than 30 Philippine Island natives were confined in a small house, threatened with deportation, their passports and transportation tickets confiscated, forced to work at low-paying jobs theoretically

to discharge debts involved in bringing them to the U.S. for a better life. Accumulating charges for their board ensured they never were free of the debt.

In South Hillsborough County last weekend, sheriff's deputies and U.S. Border Patrol agents intercepted two women transporting five Mexican nationals illegally in this country and enroute to farms in Immokalee, ostensibly for jobs and wages, quite possibly for another outcome.

In the first instance, charges under Florida's human trafficking statute have been lodged against three pimps. In the second, a husband and wife team operating so-called employment agencies was charged with a number of offenses from trafficking to fraud, and convicted. In the new South Hillsborough case, a drug charge has been filed and a human trafficking filing is pending as one of the women carrying $6,000 in cash resides for the moment in a Hillsborough jail. Border patrol agents took custody of the currency and the vehicle.

This is 21st century human trafficking. And Florida is in the thick of it, one of three primary U.S. human trafficking destinations. Its climate, beaches and landscape make attractive lures used to entice victims then isolated and made increasingly vulnerable by their captors, enslaved by physical, verbal and other abuses.

It targets populations least able to defend themselves – children, runaways, attractive women in need, foreign adults desperate for a chance in the U.S. It is linked to pornography and to organized crime. It is largely a cash business, and lots of it.

It's a brutal, ugly, inhumane business with a long history. Prehistoric artifacts indicate that enslavement of and trade in human beings goes back to the hunter societies. Americans began taking an interest in "white slavery" — trafficking in women and girls – a hundred years ago, passing the country's first laws prohibiting the practice. Today, task forces exist to inform the general public, advocate for tougher laws and provide for rescued victims.

It still happens, though, and the efforts of one of them focused on South Hillsborough in late January, human trafficking awareness month. Using a workbook developed by the Florida Regional Community Policing Institute at St. Petersburg College, members of the Clearwater Area Taskforce on Human Trafficking conducted a four-hour seminar for interested South County citizens. The taskforce covers Pinellas, Pasco and Hillsborough Counties.

Dewey Williams, a retired deputy police chief, and Sandra Lyth, chief executive of the Intercultural Advocacy Institute in Pinellas, took turns explaining "the many faces of human trafficking," how it functions in Florida, the profits realized by its perpetrators and the toll taken in human lives. They were joined by Hilary Sessions, mother of Tiffany Sessions, the 20 -year-old University of Florida student who disappeared without a trace 23 years ago this month in Gainesville. The economics major's abduction case remains open and the search for her continues as authorities consider she could have become a human trafficking victim.

For profit-making organized crime, human trafficking is second only to the drug trade, Williams and Lyth emphasized, producing an annual return to all perpetrators estimated at $32 billion. It is becoming the preferred business activity for crime syndicates around the world, they added. And on a worldwide basis, some 12 million people are in forced labor and forced prostitution, they said.

Victims often are "invisible," perhaps in the U.S. illegally, kept physically isolated and guarded, the speakers said. They may be unable to use English, may not know where they are located and may face many cultural barriers, unaware that they have rights under American law.

They are controlled by their captors with a wide range of abuses, including beatings, burnings, rape, starvation, drug and alcohol dependency as well as threats aimed at their families, debt bondage and loss of documents proving their identities, origins and other vital information.

Victims can be found working not only in prostitution,. exotic dancing and adult clubs, but also as maids in hotels, in restaurant kitchens, in domestic service, in factories, on landscape crews and in agricultural packing plants or fields, plus as day laborers, on carnival midways and begging on public streets.

They once may have been among the millions of homeless youngsters roaming America's cities or among the many girls and women who disappear from their home ground every year for no apparent reason or from an impoverished country where the only chance for improvement in circumstances is escape. What they have in

common are needs, dreams, ambitions that can be exploited, Williams and Lyth noted.

However, victims sometimes can be spotted, they also said. Human trafficking victims may lack personal items and possessions, may be without financial records and personal documents, may not have transportation or knowledge of the community. They may appear malnourished, have injuries from beatings or weapons and show signs of branding or torture. They also may be overseen by a third party who insists on interpreting or holding legal and travel documents.

As the three-county taskforce now focuses on South Hillsborough, plans are taking shape for a number of awareness programs and fund-raising projects with a range of objectives, according to June Wallace, a Kings Point resident and taskforce member.

In the near term, legislation tightening Florida's human trafficking law – contained in SB 1880 – is making its way through the process in Tallahassee at this time, three billboards showing a man and the message "he wants to rent your daughter" are planned along interstate roadways during the August GOP convention and a WRAP – White Ribbons against Porn – campaign is set for the first week in November.

The local committee being chaired by Wallace also is putting together a speakers' bureau to provide programs for local organizations as the men's group at the United Methodist Church in Sun City Center is initiating a mentoring program for its boy scouts. In addition, an eight-hour training course for local law enforcement officers is being coordinated with sheriff's office schedules.

From a longer perspective, Wallace said the groundwork for an ARTreach program as an after-school activity for middle and high school girls now is underway. The objective is to conduct classes after school hours and probably under the aegis of one of the local churches in graphic and dramatic arts designed to educate girls in avoiding human trafficking pitfalls. Supplies are being collected.

And one of the longest range goals is development of a safe retreat for rescued trafficking victims in Central Florida, she added. Such a sheltered environment exists in Georgia, using equine therapy in a ranch-like setting to promote the emotional and psychological healing required for the trafficking victim's successful journey back to constructive, independent living. This goal has been undertaken by a St. Petersburg-based organization called "Bridging freedom" dedicated to "restoring stolen childhoods" by finding "Solutions for Domestic Minor Sex Trafficking Victims."

Wallace's South County committee will be helping with fund raising for the retreat development, beginning with an event dubbed "Chair-aTea" foreseen on a Sunday in early 2013, she said. The event is to feature an especially blended tea, along with assorted delicacies, served to tables of eight, she added. The event also will include a silent auction of donated novel and unique handbags "filled with goodies" in a feature called "Purses for a Purpose."

Yet another highlight of the event is to be a live auction of one-of-a-kind chairs created and donated by local artists. Wallace said she anticipates the chairs will materialize in the months before the slated tea so they can be displayed and viewed in prominent South County locations prior to the bidding opportunity.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Report: Super Bowl Fans Possibly Exposed To Measles In Indianapolis

Boston/CBS Local
February 8, 2012

The cost for fans to attend the Super Bowl is sky-high, but possible exposure to measles could make the price much higher than anyone expected.

According to WISH-TV in Indianapolis, the Department of Health is investigating whether a person with the contagious disease visited the Super Bowl village on Friday. Two people have since contracted measles.

Measles is a highly contagious illness that can be spread through the air by coughing or sneezing.

Symptoms include a high fever, runny nose, watery red eyes and a cough, followed days later by a rash.

Those who notice symptoms are encouraged to contact their doctors.

Anita Barry of the Boston Public Health Commission told WBZ-TV they are aware of the situation, but have not had any reports of measles cases here.

Barry said if you believe you have symptoms call your doctor, but don't go in, in the event you may be infected.

[Return to top] *Topic Area: Public Health & Healthcare*

Chicken Salad Sandwiches Another Egg-Related Recall

Food Safety News
February 8, 2012

Grand Strand Sandwich Company of Longs, SC is recalling some of its chicken salad sandwiches from convenience stores in the Southwest after its distributor recalled the chicken salad used to make them.

The recall is the latest in the string of recalls that began January 26 when Michael Foods revealed that some of its hard-cooked eggs could be contaminated with Listeria.

No illnesses have been associated with the hard-cooked eggs distributed by Michael Foods or any of the products made with the eggs.

In a news release Wednesday, Grand Strand wrote that its recall "came about when Bost Distributing, our chicken salad manufacturer, bought some of the hard-cooked eggs that were produced (and later recalled) by Michael Foods. Bost Distributing was unsure if the eggs from Michael Foods were used in our product, so just to be safe we are recalling (the sandwiches)."

The recalled sandwiches include:

- Grand Strand Sandwich 4.5 oz., UPC 067068101056, sell-by 02/24/12
- Grand Strand Sandwich 4.5 oz., UPC 067068101056, sell-by 02/29/12
- Country Harvest Chicken Salad 5 oz., UPC 067068171059, sell-by 02/23/12
- Lunchbox Chicken Salad 4.5 oz., UPC 067068121050, sell-by 02/24/12

[Return to top] *Topic Area: Public Health & Healthcare*

Alleged JPL Computer Hacker Indicted [CA]

By Bill Kisliuk
Pasadena Sun/Los Angeles Times
February 8, 2012

A Romanian man who allegedly hacked into Jet Propulsion Laboratory computers and interfered with NASA satellite research was indicted this week by a federal grand jury.

Robert Butyka, 25, who prosecutors say used the moniker "Iceman," is accused of hacking into 25 computers at JPL in La Cañada Flintridge in December 2010 and interfering with the Atmospheric Infrared Sounder Program, according to the U.S. attorney's office in Los Angeles.

Authorities said the hack cost NASA $500,000 — including down time — to wipe an implanted code from the system.

As of Wednesday, Butyka described himself online as being a "computer security tester" in Cluj, Romania, and that the firm he worked at was interested in "ethical hacking."

Butyka was convicted in Romania of charges related to the alleged JPL hack following a joint investigation with U.S. authorities, according to federal prosecutors. He was sentenced to a three-year prison term in the Eastern European country, where the alleged hacking took place.

Atmospheric Infrared Sounder Program instruments fly on a satellite called Aqua, according to NASA, and are designed to measure climate change indicators, such as greenhouse gases and water vapor.

The system has been in operation since 2002 and can generate as much information as 300,000 individual weather balloons sent up from sites around the world, according to the space agency. The instruments also study the role of clouds in affecting temperature and distribution of greenhouse gases.

JPL researchers could not use computers tracking the program's data for two months while experts removed the malicious software, according to the U.S. attorney's office. NASA's Office of the Inspector General in Washington, D.C., conducted the probe.

JPL spokeswoman Veronica McGregor said the agency does not comment on security details. "We are pleased by the efforts that have been taken to resolve the case," she said in a statement.

If convicted of intentionally interfering with transmission of information in the United States, Butyka faces up to 10 years in U.S. federal prison.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Wyola Man Admits Eagle Trafficking [MT]

By Clair Johnson
Billings Gazette
February 8, 2012

Wyola resident Ernie Lemuel Stewart admitted Wednesday that he baited eagles, killed them and sold their carcasses for thousands of dollars.

Stewart, 33, pleaded guilty in U.S. District Court in Billings to two counts of unlawful eagle trafficking, a felony. Two other counts are to be dismissed under the terms of a plea agreement.

Stewart and at least five others were indicted last year on eagle and migratory bird trafficking violations after a three-year investigation by the U.S. Fish and Wildlife Service called Operation Rolling Thunder.

Stewart also pleaded guilty last month in South Dakota to illegally selling eagle parts in Spearfish as part of the same investigation.

Assistant U.S. Attorney Mark Steger Smith said in court records that Stewart sold eagle carcasses and parts to an informant and also to the informant through a middleman, Gilbert G. Walks Jr. Walks, 49, of Crow Agency.

Walks pleaded guilty last week to eagle trafficking charges.

Stewart told the informant the eagles were hard to get because of "the law and everything," Steger said. Stewart hunted the eagles by baiting them with deer ribs near Aberdeen, which is south of Wyola on the Crow Reservation, and shooting them, he said.

Stewart also was the supplier in a February 2010 deal brokered by Walks in which the informant bought five whole eagle carcasses, including two bald eagles, for $2,000, Steger said.

Eagles are protected under the Bald Eagle and Golden Eagle Act as well as under the Migratory Bird Species Act, which protects other bird species.

American Indians are allowed to have eagle parts and feathers for use in religious ceremonies but must apply for a permit from FWS.

The agency manages the National Eagle Repository, which accumulates eagle carcasses and parts and distributes them to permit holders.

Stewart faces a maximum of one year in prison and a possible $5,000 fine.

Senior U.S. District Judge Jack Shanstrom set sentencing for May 9 and continued Stewart's release.

Others pleading guilty in the investigation include William Esley Hugs Jr., of Crow Agency, to five felonies; and his uncle, Harvey Allen Hugs, of Hardin, to a misdemeanor.

[Return to top] *Topic Area: Illegal Animals & Animal Products Trafficking*

Hacker Group 'Anonymous' Tried To Extort Payment From Symantec

By Steven D. Jones
Dow Jones News wires/The Wall Street Journal
February 8, 2012

Symantec Corp. (SYMC) is bracing for the release of more purloined source code in coming weeks following the disclosure that an individual claiming to be part of "Anonymous" attempted to extort payment from the company in exchange for not making the code public.

The loose-knit computer-hacking group Anonymous posted a string of emails this week purporting to show Cupertino, Calif.'s Symantec engaged in negotiations with the group to avoid disclosure of the code. Symantec spokesman Cris Paden said the email exchange took place between Anonymous and law enforcement agents, not the company.

Last month, the group published source code stolen in 2006 for Norton Utilities and pcAnywhere. The company anticipates Anonymous will next publish code for the 2006 version of Norton Antivirus Corporate Edition and Norton Internet Security.

"As we have already stated publicly, this is old code," Paden said. "And Symantec and Norton customers will not be at an increased risk as a result of any further disclosure related to these 2006 products."

Norton Antivirus is the leading product in Symantec's $2 billion consumer-software business. It is used by 150 million customers world-wide.

The conflict began a month ago, when Anonymous posted on the Web a Symantec description of how Norton Antivirus worked. Symantec said the 2,700-word document was a general description of the software from 12 years ago and didn't threaten security.

A day later, the group posted software code, which Symantec confirmed was for 2006 versions of enterprise security products.

Around the same time, an individual claiming to be part of Anonymous approached Symantec "saying that if we provided them with money, they would not post any more source code," Paden said. At that point, the company turned over the investigation to law enforcement. Because the investigation is ongoing, the company declined to name the agencies involved.

In its original post to the website Pastebin.com, Anonymous maintained it discovered the information in a hack of India's military computer network. Symantec has declined to comment on where the group found the source code, however, Paden said the company hasn't shared source code for its products with Indian officials.

Last week, Symantec offered free upgrades of pcAnywhere to users of the software who didn't have a version current enough to accept the most recent security updates. The company continues to recommend customers use the most current security products available to ensure protection against threats.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

Jacksonville Group Rescues Human Trafficking Victims [FL]

First Coast News
February 8, 2012

On the streets of Jacksonville lurks a dangerous network of human trafficking.

Many are runaway teens, some under the age of 14. Others have been shipped to the U.S. All are being sold for sex.

"There's ways for them to contact us, and if they are ready to run we will send a team after them," said Dan Benedict, the founder of what is called the Defender Foundation.

Benedict has a history himself. "I had an internet pornography addiction a while back myself, and it destroyed my life and my family." His past now has him on a mission: to give hope.

The Defender Foundation is a volunteer group in Jacksonville which hunts for victims of human trafficking across the world.

"Some major groups are behind this. Various bike gangs, Russian organized crime," said Benedict.

The group has been up and running for one year. It's now working with local Russian churches to track down victims.

"We have trafficking victims coming in from various ports in cargo containers drugged for that journey and then sold up the east coast," said Benedict.

He also notes his group has traveled from Jacksonville to Pennsylvania, the Dominican Republic and so far has helped rescue 15 girls in 10 different operations.

"I'm one of the first people that connects with them, make conversation and make them feel safe," said Erin Pruett.

Pruett is part of an all woman team in the Defender Foundation who has gone through combat training. Her job is to make contact and help the girls escape.

"You can't do everything for everyone. You can't rescue everyone, but you can do for one what you wish you could do for everyone, and that's how I take it," said Pruett.

Those with the Defender Foundation said the recovery process can be dangerous, but they are prepared for it.

"There's a security team. Their goal is to be there within five seconds if there are any problems," said Benedict.

While the Defenders don't work in conjunction with police, they do pass along information to authorities.

"We are not out there being cowboys and kicking down doors," said Benedict. He says his group has been met with some resistance by authorities.

Benedict said the Defender Foundation follows the law at all times. And if a rescued victim suddenly decides they don't want to leave, "We are not kidnappers, we're going to have to let them off," said Benedict.

There's no way to tell how many are trapped inside the dangerous web of human trafficking. It's so rampant, authorities can't even keep track.

That's why the Defender Foundation is focused on its mission to deliver hope to those in need of rescue.

"We could rescue every girl in the planet tonight. Tomorrow the demand is so huge that hundreds of thousands would be taken," said Benedict.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Judge Allows Secret Surveillance Evidence In July Trial Of Iraqi On Terrorism Charges In Ky.

By Brett Barrouquere
Associated Press
February 8, 2012

Secret documents suggest an Iraqi man facing charges of trying to funnel weapons and cash to al-Qaida operatives in his home country was "an agent of a foreign power," and his lawyers may not see or suppress those documents, a judge ruled Wednesday.

U.S. District Judge Thomas B. Russell set a July 30 trial date during a conference call with prosecutors and an attorney for 24-year-old Mohanad Shareef Hammadi, who faces charges of attempting to provide material support to terrorists and terrorist organizations and conspiracy to transfer surface-to-air missile launcher systems.

Russell ruled that prosecutors acted properly in gathering physical evidence and conducting electronic surveillance of Hammadi under the Foreign Intelligence Surveillance Act. Russell also ruled that Hammadi's attorneys may not have access to the warrants or supporting materials.

After reviewing documents submitted by prosecutors, Russell concluded that there's probable cause to believe Hammadi was "an agent of a foreign power."

"Thus, Hammadi's arguments based on the Government's failure to demonstrate probable cause are without merit," Russell wrote in a 19-page ruling.

Hammadi's co-defendant, 30-year-old Waad Ramadan Alwan, pleaded guilty in December to the same charges that Hammadi faces, as well as conspiracy to kill U.S. nationals abroad, conspiracy to use a weapon of mass destruction against U.S. nationals abroad, and distributing information on how to make and use improvised explosive devices. His sentencing is set for April 3.

Russell ruled in September that Alwan and Hammadi could be tried in civilian court, a matter that has escalated into a hot political issue.

Senate Minority Leader Mitch McConnell pushed to have Alwan and Hammadi tried at the military-run prison at Guantanamo Bay. U.S. Attorney General Eric Holder has said terrorism-related trials can be successfully handled by civilian courts.

Hammadi's attorney, James Earhart of Louisville, sought to get access to and exclude the evidence obtained under the Foreign Intelligence Surveillance Act. Russell found that the warrants were properly issued.

"The FISA materials pertaining to Hammadi will not be disclosed or suppressed," Russell wrote.

Russell's ruling on evidence does not disclose what investigators found out about Alwan and Hammadi, nor does it say how the information was gathered. The warrants issued by the Foreign Intelligence Surveillance Court during the investigation remain under seal.

Keeping such evidence hidden from public view — and even from the defendants — is routine, said Frank Cilluffo, director of the Homeland Security Policy Institute at George Washington University and a former special assistant for homeland security for President George W. Bush.

"It's a means to protect classified information," Cilluffo told The Associated Press.

Charles Rose, a Stetson University School of Law professor and former U.S. Army intelligence officer, said evidence obtained under FISA doesn't often crop up in civilian cases.

"That's a big change," Rose said. "It really hasn't been challenged."

Alwan and Hammadi entered the United States through a refugee program in 2009. Investigators matched a thumbprint from an unexploded improvised explosive device in Iraq to Alwan as part of the probe.

Both have remained in federal custody since their arrests.

[Return to top] *Topic Area: Terror Investigations and Trials*

Weekly Illicit Commercial Goods Report - 09 Feb 12

Download file

[Return to top] *Topic Area: Weekly DHS Illicit Commercial Goods Report*

Daily Infectious Diseases Report - 09 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Infectious Diseases Report*

Daily Human Trafficking Report - 09 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Human Trafficking and Smuggling Report*

Daily Terrorism Report - 09 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Terrorism Report*

Daily Cyber Report - 09 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS Cyber Report*

Daily Infrastructure Report - 09 Feb 12

Download file

[Return to top] *Topic Area: Daily DHS IP Report*

UNCLASSIFIED

From:	OSINT Branch Mailbox
To:	OSINT Branch Mailbox
Subject:	DHS-OSE Homeland Security Central Digest - 2012-03-23
Date:	Friday, March 23, 2012 6:54:53 AM
Attachments:	DHS Daily Digest - 20120323.pdf

Classification: UNCLASSIFIED

(U) The DHS Homeland Security Central Digest for 23 March 2012 is attached.

(U) Redistribution is encouraged. Please feel free to forward this email w/attachment to your co-workers and colleagues that might be interested in this product.

(U) This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats to the homeland. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures.

(U) Articles and resource documents come from open source information and are posted to the Homeland Security Central website on Intelink-U. For information on establishing an Intelink-U account, please visit http://ra.intelink.gov.

(U) The Homeland Security Central Digest contains full article text and may contain copyrighted material whose use has not been specifically authorized by the copyright owner. This information is available to DHS, in the interest of illuminating incidents and events that may have an impact on national security and critical infrastructure protection. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.

(U) This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted.

(U) Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: (b) (6)

(U) This product can also be viewed at the Homeland Security Central website on Intelink-U at: https://www.intelink.gov/hls/.

Regards,
- - - - - -
Open Source Content Management
Department of Homeland Security

E-mail: (b) (6)

Classification: UNCLASSIFIED

DHS Open Source Enterprise
Daily Digest
23 March 2012

Authorities Seize $275,000 In Unreported Cash At Mexico Border [AZ]
Customs and Border Protection officers reportedly seized nearly $275,000 of unreported U.S. currency Tuesday from two individuals traveling to Mexico through the Mariposa port. [HSEC-4.10]

Mexico, Awash In Weapons, Has Just One Legal Gun Store
Mexico has some of the most restrictive gun laws in the world. That, however, hasn't stopped Mexicans from acquiring firearms. The country is awash in illegal guns, many of them assault weapons in the hands of merciless criminal gangs. [HSEC-10.7]

South Florida's Taste For Conch Drives Smuggling, Black Market Sales
State and federal wildlife authorities are investigating a network of suspected conch-smuggling rings that traffic hundreds of pounds of sea snail from the Bahamas to satisfy South Florida appetites. [HSEC-4.10]

Authorities Probing Possible Terrorist Links To People Taking Photos Of NYC Landmarks
Authorities have interviewed at least 13 people since 2005 with ties to Iran's government who were seen taking pictures of New York City landmarks, a senior New York Police Department official said yesterday. [HSEC-8.3]

Mexican Gun Traffickers Busted In McAllen Sent To Prison [TX]
A federal judge sent two illegal immigrants to prison for their roles in a gun trafficking ring busted on the city's northwest side. Authorities recovered five assault rifles and a pistol from four illegal immigrants at 3512 Violet Ave. in February 2011. [HSEC-10.10]

Meth Lab Suspects Indicted [OH]
Four Scioto County men arrested last month in Hanging Rock for allegedly operating a mobile methamphetamine lab were indicted this week by the Lawrence County Grand Jury. A Kentucky man who allegedly admitted to authorities he came to Ironton to have sex with an underage girl was indicted as well. [HSEC-5.10]

Waltham Man Arrested For Serious Gun, Drug Charges [MA]
A Waltham man was arrested last weekend on a slew of serious drug and weapons charges. Kamil Messac-Sylvain, 21, of 13 Hartwell St., faces 15 serious charges stemming from police finding cocaine, marijuana and two firearms in his dwelling. [HSEC-5.10]

Lawsuit Alleging Bank Of China Laundered Terrorists' Money Moves Forward
The Bank of China knowingly laundered money for various Islamic militant groups so they could get around transaction restrictions because of their label as a "terrorist organization" by the U.S. government, a lawsuit by Israeli victims of suicide bombings claims. Recent court decisions in the United States say the lawsuits can go forward against the Chinese bank. [HSEC-8.8]

Verizon Study Confirms 2011 Was The Year Of Anonymous, With 100 Million Users' Data Breached By Hacktivists
In 2011, hacktivists made their presence felt in the world of information security more than ever before, and by some measures even more than the financial criminals who usually dominate data breach statistics. [HSEC-1.2]

U.S. Visas Available For Trafficking Victims
The U.S. Citizenship and Immigration Services office in Long Island City hosted a forum Tuesday to get the word out about legal options for immigrants who have been victims of human trafficking, abuse or domestic violence. [HSEC-3.10]

ICE: Man Used Craigslist To Recruit Human Smugglers
Federal authorities arrested a Mexican national accused of using Craigslist to recruit "coyotes" for his human smuggling operation. [HSEC-3.10]

Pesticide Pulled From US Market Amid Fear Of Toxicity
A manufacturer has pulled a controversial pesticide from the American market, surprising both growers and environmentalists who have warned that it poses serious hazards. [HSEC-6.1]

Full Text of all new articles....

Authorities Seize $275,000 In Unreported Cash At Mexico Border [AZ]

By Brenna Donnelly
CBS 5 Arizona
March 21, 2012

Customs and Border Protection officers reportedly seized nearly $275,000 of unreported U.S. currency Tuesday from two individuals traveling to Mexico through the Mariposa port.

Officers pulled over Jorge Javier Velasco's Volkswagen sedan for inspection and additional questioning and reportedly found the unreported cash wrapped in 18 packages hidden under the car's main frame.

Velasco, 52, of Nogales, AZ, was arrested along with his passenger, 40-year-old Maria Luisa Ramirez-Cota of Nogales, Sonora, Mexico. Both were turned over to U.S. Immigration and Customs Enforcement's Homeland Security Investigations.

[Return to top] *Topic Area: Currency Trafficking & Money Laundering*

Mexico, Awash In Weapons, Has Just One Legal Gun Store

By Tim Johnson
McClatchy Newspapers
March 21,2012

Mexico has some of the most restrictive gun laws in the world. If any of the nation's 112 million citizens want to buy firearms, there's only one store where they can do it legally. It's on a sprawling military base and run by the army.

That, however, hasn't stopped Mexicans from acquiring firearms. The country is awash in illegal guns, many of them assault weapons in the hands of merciless criminal gangs. President Felipe Calderon says authorities have seized more than 140,000 weapons since he came to office in late 2006. Many of them, Mexican officials assert, were purchased in the United States.

Nothing highlights the cultural and legal differences between Mexico and the United States as starkly as Mexico's lone gun shop, whose ponderous name is the Directorate of Arms and Munitions Sales.

In contrast, the four U.S. border states -- California, Arizona, New Mexico and Texas -- have 20,834 firearms dealers licensed by the U.S. government, according to Marc Willis, a spokesman for the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives.

In the gun shop here, soldiers keep a wary eye on customers as they pass through a metal detector. Once inside, clients seeking protection for their homes are each permitted to buy one small-caliber handgun. They also can obtain 200 rounds of ammunition a year.

"Normally, we have 70 or 100 visitors a day," army Col. Raul Manzano Velez said as he took a visitor past rows of wooden cabinets displaying Belgian-, German-, Turkish- and U.S.-made handguns and single-shot hunting rifles.

The shop's existence is unknown to many citizens. "The federal firearms law forbids us from advertising so as not to promote rampant gun buying," Manzano said.

Despite the rigor of Mexico's gun laws, its murder rate of 18 per 100,000 people is more than triple the United States' rate of five per 100,000. Nearly all homicides in Mexico occur with firearms.
Mexico once had a few private gun shops but the last one was abolished in 1995, leaving business to the army store. Profits go to the national treasury.

Obtaining a gun involves first getting a permit. Requirements include an official photo ID, proof of residency and employment, a document showing fulfillment of military service and a declaration of a clean criminal record.

"When you have all these documents, you take them to the federal firearms registry, and within five to 10 working days you get the license," Manzano said.

For those seeking guns for home protection, the law requires that the firearms never leave the permit holders' primary residences. The firearm can be from .22 to .380 caliber. It can be a pistol or a revolver, but can't be a rifle. Only a single gun is allowed.
A different permit is given to marksmen and hunters, allowing them each to own up to nine single-shot rifles or shotguns and one small-caliber handgun. Mexico has 89 gun and hunting clubs and 20 government offices that sell hunting licenses.

Mexico's 289 private security companies also have a different regimen: They can buy semiautomatic weapons or higher-caliber pistols and revolvers.

No matter how far buyers live from Mexico City, they must travel to the capital to obtain the licenses, give fingerprints and purchase the weapons.

Manzano acknowledged that the system is "very inconvenient" for the buyer, especially given the underground market for weapons.

"There is an enormous black market in the country. You can buy any weapon without any problem on the street. That is the reality in Mexico," he said.

[Return to top] *Topic Area: Weapons Trafficking*

South Florida's Taste For Conch Drives Smuggling, Black Market Sales

By Alexia Campbell
Sun Sentinel
March 22,2012

State and federal wildlife authorities are investigating a network of suspected conch-smuggling rings that traffic hundreds of pounds of sea snail from the Bahamas to satisfy South Florida appetites.

High demand for the protected species — long over-fished in Florida waters — fuels black market sales that smugglers use to evade international rules regulating commercial trade of queen conch. The practice is depleting the Bahamian conch population, experts say, and putting unsuspecting consumers at risk of illness.

At least six people have been indicted in South Florida in the past year for illegally importing conch.

The cases point to a larger, organized network of people who profit from trafficking the seafood delicacy to South Florida, said Lt. Steve Arcuri of the Florida Fish & Wildlife Conservation Commission. They buy it on the black market at $4 a pound in the Bahamas, he said, and sell it to local restaurants and markets for up to $16 a pound, which is below market price here.

"There's money to be made," said Arcuri. "It's like drug smuggling. If they think they can get away with it, they'll continue doing it."
In February, an illegal load of conch — worth about $25,000 — was intercepted by federal customs agents near the Jupiter Inlet. Robert Fortunato, 55, and Mark Kulbacky, 56, had 1,500 pounds of frozen conch hidden in their sportfishing boat, according to a federal indictment filed in West Palm Beach.

The pair bought the conch from a man in the Bahamas and planned to resell it in South Florida, the indictment said. Both men face up to 10 years in prison if convicted of illegally importing wildlife and conspiring to illegally import wildlife.

Fortunato faces up to five years more if convicted of lying to customs officials.

In September, a Palm Beach County man avoided prison time after he was caught with 343 pounds of conch contraband. Van Bodden-Martinez, 48, pleaded guilty in federal court to illegally importing wildlife from the Bahamas and was sentenced to three years probation.

U.S. demand for conch delicacies is largely to blame for over fishing and illegal sales, federal authorities said. By 1985, most of Florida's conch had been plucked from its shallow waters, leading to a statewide ban on conch fishing. The United States now is the largest consumer of imported conch, buying more than 80 percent of the conch available for international trade.

Ron Messa, a special agent with the National Oceanic and Atmospheric Administration in Miami, said he's sees more people try to skirt international laws to meet that demand. But it could endanger consumers, he said.

"It could be a potential health issue," Messa said. "We don't know how [the conch] is being handled in the Bahamas."

The FDA requires conch exporters to develop procedures that ensure conch is not contaminated with salmonella and paralytic shellfish poisoning toxins. If it gets into the country illegally, there is no safeguard, an agency spokesman said.

Owners of local seafood markets and restaurants are frustrated to see competitors get a steady conch supply for less money, said Peter Longchamp, account manager for Mr. Fish in Pompano Beach.

"When you take shortcuts like that, it ends up hurting honest businesses who go through all the paperwork," he said.

[Return to top] *Topic Area: Counterfeit Goods & Illegal Commercial Trafficking*

Authorities Probing Possible Terrorist Links To People Taking Photos Of NYC Landmarks

The Associated Press
March 22,2012

Are these camera-toting people harmless tourists? Or potential terrorists?

Authorities have interviewed at least 13 people since 2005 with ties to Iran's government who were seen taking pictures of New York City landmarks, a senior New York Police Department official said yesterday.

Police consider these instances to be pre-operational surveillance, bolstering their concerns that Iran or its proxy terrorist group could be prepared to strike inside the United States, if provoked by escalating tensions between the two countries.

Mitchell Silber, the NYPD's director of intelligence analysis, told Congress that New York's international significance as a terror target and its large Jewish population make the city a likely place for Iran and Hezbollah to strike. Silber testified before the House Homeland Security about the potential threat.

Much of what Silber said echoed his previous statements on the potential threat, but he offered new details yesterday about past activities in New York.

In May 2005, Silber said, tips led the NYPD to six people on a sight-seeing cruise who were taking pictures and movies of city landmarks like the Brooklyn Bridge. In September 2008, police interviewed three people taking pictures of railroad tracks.

And in September 2010, federal air marshals saw four people taking pictures and videos at a New York heliport. Interviews with law enforcement revealed that all were associated with the Iranian government, but they were ultimately released and never charged, Silber said.

U.S. officials long have worried that Iran would use Hezbollah to carry out attacks inside the United States. And Iran was previously accused in a disrupted plot to assassinate the Saudi ambassador to the U.S. here last year, a plan interpreted in the U.S. intelligence community as a clear message that Iran is not afraid to carry out an attack inside this country.

In January, James Clapper, the top U.S. intelligence official, said some Iranian officials are probably "more willing to conduct an attack in the United States in response to real or perceived U.S. actions that threaten the regime."

But government officials have said there are no known or specific threats indicating Iranian plans to attack inside the U.S.

[Return to top] *Topic Area: Suspicious Events*

Mexican Gun Traffickers Busted In McAllen Sent To Prison [TX]

By Jared Taylor
The Monitor
March 21, 2012

A federal judge sent two illegal immigrants to prison for their roles in a gun trafficking ring busted on the city's northwest side.

Authorities recovered five assault rifles and a pistol from four illegal immigrants at 3512 Violet Ave. in February 2011.

A Texas Department of Public Safety investigator had received information that the house was possibly used by illegal immigrants smuggling guns to Mexican drug cartels, a criminal complaint states.

Authorities recovered three .308-caliber rifles with obliterated serial numbers, a Glock 9 mm pistol and two AR-15-style assault rifles during raids at the house and an apartment at 1116 N. 20th St., McAllen.

U.S. District Judge Randy Crane sentenced Carlos Rios Davila and Marco Guzman Velasquez at a hearing Wednesday in McAllen.

Both men received 63-month prison sentences for their roles in the gun trafficking scheme.

Crane said it was unclear whether Rios or Guzman — both illegal immigrants from Mexico — played a larger role in the gun trafficking scheme.

"I would like the United States of America to forgive me, and of course, I would like the judge to forgive me," Rios said in the courtroom in Spanish. "That is all I would like to say."

Velasquez said he wants to use his prison time for a fresh start.

"I will not come back," he told Crane in Spanish. "I would like the court to send me to a prison with educational opportunities so I can better myself."

Both men will be deported upon completing their prison time.

Also formally charged in the case were Ismael Rivera Melendez and Ferdinando Guillen Rivera; however, both men's cases were dismissed in August 2011.

[Return to top] *Topic Area: Weapons Trafficking*

Meth Lab Suspects Indicted [OH]

Ironton Tribune
March 22, 2012

Four Scioto County men arrested last month in Hanging Rock for allegedly operating a mobile methamphetamine lab were indicted this week by the Lawrence County Grand Jury. A Kentucky man who allegedly admitted to authorities he came to Ironton to have sex with an underage girl was indicted as well.

Randy Stevens, 42, of 1513 Sixth St. Portsmouth, Charles Price, 40, of 2121 Vermont Ave., Portsmouth, Danny Brown, 43, also of 2121 Vermont Ave., Portsmouth, and Charles Bond, 49, of 2842 State Route 335, Portsmouth, were each indicted on charges of illegal manufacture or production of methamphetamine, illegal assembly or possession of chemicals for the manufacture of meth and possession of criminal tools. Bond was also indicted on one count of possession of a drug abuse instrument.

In late February, the four men were stopped by a Hanging Rock Police Officer who noticed some things about the vehicle he thought were suspicious. A search of the truck allegedly confirmed the officer's suspicions and the four men were arrested.

Also, Daniel Preston Jr., 20, of 1053 Collins Ave., Ashland, was indicted on one count of importuning.

Preston allegedly met a 13-year-old female on the Internet and arranged to meet her in person late last month, authorities said. But when he showed up in Ironton and could not find the girl's address, he asked an Ohio State Highway Patrol Trooper for assistance.

The trooper became suspicious of Preston's story and took him to the Ironton Police Department for questioning. It was then Preston allegedly admitted he knew the girl was only 13 and that he had come to Ironton to have sex with her.

According to information from the office of Lawrence County Prosecutor J.B. Collier Jr., others indicted were:

• Gary A. Thomas, 42, 904 Fourth St. E., South Point, one count of having a weapon under a disability and three counts of aggravated trafficking in drugs.

• James Costello, 20, 28 Township Road 1430, Apt. 19, South Point, failure to comply with the order and signal of a police officer.

• Bobby Effingham, 30, 403 Fourth St. E., South Point, failure to comply with the order and signal of a police officer.

• Jeffrey Row, 28, 198 Township Road 1106, Proctorville, one count each of forgery and receiving stolen property.

• Anthony Workman, 34, 48 Private Drive 286, Chesapeake, unauthorized use of a motor vehicle.

• Roger Meadows, 34, 3826 Stanton Ave., New Boston, one count of having a weapon under a disability and one count of improperly discharging a firearm into a habitation.

• Teresa Wicker, 51, 484 Township Road 44, Ironton, felonious assault.

• Kenneth Smith, 47, 825 S. 10th St., Ironton, trafficking in marijuana.

• Clifford Roberts, 35, 1097 County Road 1, South Point, one count each of domestic violence, assault on a peace officer and disrupting a public service.

• Curtis Adkins, 34, 103 Kelly Lane, Chesapeake, one count each of identity fraud and receiving stolen property.

• James Shuff, 30, 2580 County Road 210, Waterloo, improperly handling a firearm in a motor vehicle.

Additionally, the grand jury also returned two secret indictments for drug offenses.

[Return to top] *Topic Area: Illegal Drug Trafficking*

Waltham Man Arrested For Serious Gun, Drug Charges [MA]

By Ryan Grannan-Doll
Waltham Patch
March 21, 2012

A Waltham man was arrested last weekend on a slew of serious drug and weapons charges.

Kamil Messac-Sylvain, 21, of 13 Hartwell St., faces 15 serious charges stemming from police finding cocaine, marijuana and two firearms in his dwelling.

The incident started on Saturday, March 17 when police escorted a woman, who had a restraining order against Messac-Sylvain, to his home to collect her possessions, according to Waltham Police Detective Sgt. Joseph Guigno. It was a pre-arranged meeting under the conditions of the restraining order, which stems from a domestic situation, according to Guigno.

As the woman was collecting her belongings, she noticed a bag containing two firearms and told police, Guigno said. Officers found the guns, which were in violation of the restraining order, and called Waltham detectives to request a search warrant for the home. The restraining order requires Messac-Sylvain to surrender his weapons.

Detectives searched the home and found 26.9 grams of cocaine, 5.5 ounces of marijuana, two firearms, $4,300 cash and a scale, according to Guigno. He identified the guns as Colt .45 caliber pistol and a Davis .380 pistol. Ammunition was also found in the home.

In total, the suspect faces the following charges: three counts of assault and battery on a police officer, one count of resisting arrest, two counts of possession of a firearm without a firearm identification charges, two counts of possession of a firearm without an ID card (subsequent offense), two counts of storing a firearm improperly, one count of receiving stolen property, cocaine trafficking, a drug violation near a school (house is near Stanley Elementary School), violating an abuse prevention order and distribution of a class D drug (subsequent offense).

[Return to top] *Topic Area: Illegal Drug Trafficking*

Lawsuit Alleging Bank Of China Laundered Terrorists' Money Moves Forward

By Leland Vittert
Fox News
March 21, 2012

The Bank of China knowingly laundered money for various Islamic militant groups so they could get around transaction restrictions because of their label as a "terrorist organization" by the U.S. government, a lawsuit by Israeli victims of suicide bombings claims. Recent court decisions in the United States say the lawsuits can go forward against the Chinese bank.

Fox News has learned that Israeli intelligence officials warned the Chinese government that Iran was using Bank

of China to finance its militant networks, including providing account numbers and transaction details, only to have the Chinese turn a blind eye as the money went to make bombs that would kill dozens of civilians.

An explosion at a Tel Aviv sandwich shop in April 2006 took just a second to kill nine and injure 60.

In the moments after, it's chaos. But the families of the victims have a lifetime to suffer and consider -- exactly how a suicide attack really starts. Normally such attacks start not with a bomb but with planning -- and money. According to the son of one man killed in the 2006 Shawarma stand attack, the needed money was laundered halfway around the world by the Bank of China.

"Bank of China is the same as Islamic Jihad. Any group…is as bad as Iran for me," Tal Erez said.

What makes these allegations even more explosive is the sworn testimony of an Israeli intelligence agent who says he personally warned the Bank of China they were moving money to build bombs and pay suicide bombers who would eventually kill hundreds.

"If (Bank of China) didn't give them the instruments to transfer money, although Israel asked them to shut down these accounts, then probably my father wouldn't be murdered six years ago," Tal said.

While it has been nearly impossible to sue individual terror groups, lawyer Nitzana Darshan says going after their bankers is just as effective as arresting or killing groups' leadership.

"The suicide bomber knows that in the end of the day, after they carry out an attack, there will be someone who will be taking care of their family for the rest of their lives. It is all based on money. You cut the funding, you cut the terrorism," said Darshan.

Islamic Jihad took responsibility for the attack that killed Tal's father. The 16-year-old bomber came from the town of Jenin and blew himself up during the Jewish holy week of Passover.

Typically in suicide bombings, the bomber's family is paid between $10,000 and $25,000 by the organization that sent their loved one to kill.

The case is one of the first times, however, that Israelis are using U.S. courts to go after a financial institution for allowing transactions of this type. Darshan says the threat of civil liability for banks has already curtailed the ability of militant groups to move needed funds to buy weapons or the hearts and minds of those where they operate.

"Our goal is to block the funding. To get the terror organization beyond the banking system because if they can't wire hundreds of millions of dollars, they don't have a choice but to bring them in suitcases or smuggling through the tunnels into Gaza or to South Lebanon. And if you cut these pipelines you defiantly hurt and damage the terror organization," said Darshan.

The Bank of China refused repeated requests by Fox News for an interview or to respond directly to questions about their involvement in moving money for Islamic Jihad or the alleged warning given by Israel's Mossad Intelligence Service. Through their lawyer, the bank sent an emailed statement saying in part, "Bank of China Ltd. ('BOC') has answered the lawsuit and formally denied the plaintiffs' allegations. Since the litigation is pending, BOC will not comment to the media on it."

According to the affidavit, known Islamic Jihad and Hamas leaders in Iran wired money to a numbered Bank of China account in Guanzhoua, China, which was controlled by Said al-Shurafa, an operative of both organizations. It's alleged that al-Shurafa would then transfer the money via various means from Guanzhoua to fellow militants in the West Bank and Gaza. In all, the affidavit details transfer of more than $1.1 million.

Tal often looks back at a picture of his father, a veteran of the 1967 Israeli war. He remembers his father as a fighter – inspiration for Tal to continue the fight against the bank he now considers a mortal enemy.

"My father was a peace man, he wants peace. I want to continue his ways," he said. "I want that the people that did these terrible things will go to jail or will pay something (so) that they will not do that again. This is our way to say – father we won. This is our heritage for him.

[Return to top] *Topic Area: Currency Trafficking & Money Laundering*

Verizon Study Confirms 2011 Was The Year Of Anonymous, With 100 Million Users' Data Breached By Hacktivists

By Andy Greenberg
Forbes
March 22, 2012

Anonymous may have had a rough 2012 so far, with dozens of its most active members arrested and one of its leaders and organizers revealed as a government informant. But a quick look at the stats shows that in terms of pure information mayhem, 2011 was its most effective year yet.

On Thursday, Verizon released its annual Data Breach Investigations Report, [PDF here] the largest study of its kind, and one that delves into data from hundreds of the company's breach responses, along with those performed by law enforcement agencies including the U.S. Secret Service as well as Australian, Dutch, U.K. and Irish police. The result of this year's study is clear enough: In 2011, hacktivists made their presence felt in the world of information security more than ever before, and by some measures even more than the financial criminals who usually dominate data breach statistics.

Of the 855 breach incidents from the last year that Verizon's security team analyzed, three percent were attributed to "hacktivists." That may seem like a small proportion, but Verizon's director of security research Wade Baker says it's giant compared to the same category in previous studies, which barely created a blip on Verizon's radar last year and accounted for less than one percent of incidents. Narrow the field of victims to only large organizations, which hackers within Anonymous and its splinters target for maximum exposure, and the number of hacktivist incidents rises to 25%.

But the real impact of last year's radical hacktivism can be seen in the numbers of actual compromised records–each one representing data attached to an individual. Of the 177 million records stolen by hackers over the last year, 100 million were taken by hacktivists. The stats don't even include common hacktivist techniques like website takedowns with denial of service attacks or defacements, instead focusing only on actual data theft.

Of those data-stealing hacktivist attacks, the vast majority were the work of Anonymous or one of the movement's subgroups, says Bryan Sartin, vice president of Verizon's RISK security group. "At least three out of four were Anonymous, where a group like LulzSec or a message saying 'We are Legion' claimed credit."

Certainly hacktivism isn't a new phenomenon. The report attributes the term to the Cult of the Dead Cow hacker group from the late 1990s. But Verizon's analysts write that hackers previously limited their attacks to defacements and website takedowns, not mass data theft. "Data theft as a tool of hacktivism was one of the most damaging things they could do," says Baker. "And they were very successful at it."

Verizon doesn't break its numbers down into specific incidents, but the exploits of Anonymous, and specifically its submovements like LulzSec and Antisec over the last year certainly seem to have produced enough breaches to account for Verizon's figures. LulzSec, for instance, went on a rampage last spring that began with its dump of 73,000 names of contestants on the U.K. television show the X-Factor and followed up with hacks of Sony, a handful of video game companies, porn sites, and defense contractors. Each attack led to releases of tens or hundreds of thousands of users' information, and one package the group released of random stolen leftovers was thought to contain around 750,000 users' data.

Verizon's Baker notes that the hacktivist attacks the study analyzed show a lower number of skilled attacks on targets that produced a higher volume of stolen data when compared to the tactics of typical financially-motivated cybercriminals. Baker says profit-motivated hackers were far more likely in 2011 to attack small firms such as the franchises of retail corporations, reproducing their low-volume thefts again and again. That finding echoes the results of another report released by the security firm Trustwave earlier this year, which stated that one third of the breaches it investigated targeted franchises.

Because hacktivists were targeting larger organizations and seeking publicity rather than silent, profitable theft from easy targets, they used some tactics that Verizon says it had rarely seen before: DNS tunneling, for instance, which exploits a target's servers that convert IP addresses to domain names as an entrypoint into its

networks, or denial of service attacks that served as a distraction while the attackers simultaneously penetrated another part of the network. In close to 75% of cases, hacktivist targets were warned ahead of time that they would face an attack, a tactic that rarely if ever is used by financially-motivated hackers.

"They definitely demonstrated different modes, and in many cases a lot more sophistication," Baker says.

[Return to top] *Topic Area: Cybercrime & Cybersecurity*

U.S. Visas Available For Trafficking Victims

By Rebecca Henely
Times Ledger
March 22, 2012

The U.S. Citizenship and Immigration Services office in Long Island City hosted a forum Tuesday to get the word out about legal options for immigrants who have been victims of human trafficking, abuse or domestic violence.

"We know there are victims out there and there is help available," said Andrea Quarantillo, district director of USCIS for New York City, at the office at 27-35 Jackson Ave.

Scott Whelan, of the USCIS's office of policy and strategy, said there are three ways that can help immigrants who have been victimized.

First, T visas allow victims of all types of trafficking — forced labor, sexual or involuntary servitude — to stay and work in the United States on a temporary basis.

Whelan said many victims of this underground crime end up dead.

"Human trafficking is a brutal crime," he said.

A U visa is available for victims of abuse and other crimes, Whelan said. Immigrants who suffer from domestic violence, both female and male, also can apply for legal status without having to go through their abusive spouse under the provisions of the Violence Against Women Act.

"There are avenues for them to come forward," said Lynn Boudreau, USCIS's assistant center director for the Vermont Service Center.

Boudreau said the government issues 10,000 U visas each fiscal year and 5,000 T visas. The U visas are usually all issued, which means some cases are carried over to the next year, although the T visas are underused.

Julie Dinnerstein, a professor of immigration law, said it is hard to quantify how widespread the problem of human trafficking is in the city because there are many obstacles to enforcement.

Victims are sometimes part of international trafficking rings and they often do not come forward for fear not only about their own safety, but the safety of their families at home. She said those who have been prostituted also fear stigma.

"There's this myth of an army of voluntary prostitutes out there," she said.

Finally, Dinnerstein also said trafficking victims can come to the United States through various avenues, including tourist or student visas, through a marriage to a U.S. citizen, through a family who are permanent residents or through smuggling.

Even if requests for visas are eventually denied, Quarantillo said USCIS does not then begin deportation for the immigrant. USCIS also works closely with judges and the U.S. Immigration and Customs Enforcement if a crime victim is going through the process.

"We do not use these cases as a way to put people in removal proceedings," Quarantillo said.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

ICE: Man Used Craigslist To Recruit Human Smugglers

By Jared Taylor
The Monitor/Brownsville Herald
March 21, 2012

Federal authorities arrested a Mexican national accused of using Craigslist to recruit "coyotes" for his human smuggling operation.

U.S. Border Patrol agents arrested José Gustavo Díaz Velásquez, 29, on March 14 during an investigation into someone using Craigslist to recruit drivers to transport undocumented immigrants through the Rio Grande Valley, a U.S. Attorney's Office news release states.

The Immigration and Customs Enforcement investigation into the Craigslist human smuggling recruitment effort began last August, when agents found about 10 different postings believed to be connected to the organization.

Agents managed to locate a McAllen apartment, belonging to Diaz's wife, where the Craigslist postings originated, prosecutors said.

Díaz also had a YouTube account with a dash-cam video of a high-speed pursuit that occurred in La Joya, prosecutors said. The driver eluded law enforcement, but police said they detained nine undocumented immigrants from Díaz's vehicle.

ICE agents said they interviewed several people hired to transport immigrants, eliciting information that helped ICE build its case against Diaz.

Border Patrol agents said they arrested Díaz when they saw him near a known human smuggling area in Rio Grande City on March 14.

Diaz appeared Wednesday before U.S. Magistrate Judge Dorina Ramos in McAllen. He remains in federal custody.

[Return to top] *Topic Area: Human Trafficking & Smuggling*

Pesticide Pulled From US Market Amid Fear Of Toxicity

By Malia Wollan
New York Times
March 21, 2012

A manufacturer has pulled a controversial pesticide from the American market, surprising both growers and environmentalists who have warned that it poses serious hazards.

The soil fumigant, known as methyl iodide and sold under the label Midas, will be withdrawn immediately as a result of a review of the product's "economic viability in the U.S. marketplace," the Tokyo-based company, the Arysta LifeScience Corporation said in a statement late Tuesday.

In the five years methyl iodide has been on the market, it has seen relatively little use. Farmers have injected the pesticide into only 17,000 acres — mostly planted with tomatoes, peppers and nuts — mainly in the southeastern United States.

Although federal environmental regulators approved the pesticide in 2007, methyl iodide became a focus of fierce debate in California before it gained final approval from state regulators there in December 2010.

In hearings on the chemical, intended for use on the state's lucrative strawberry crop, scientists and environmental activists raised concerns about its neurotoxicity and its potential to cause cancer and

neurodevelopmental disorders. One member of the department's own scientific review committee called it "one of the most toxic chemicals on earth."

Still, the company's sudden removal of the product was unanticipated. "We were totally surprised by this," said Carolyn O'Donnell, a spokeswoman for the California Strawberry Commission, a growers' organization. The state's farmers grow 88 percent of the nation's strawberries, worth some $2.3 billion a year.

While the loss of methyl iodide means "one less tool in the toolbox" for strawberry farmers, Ms. O'Donnell said the industry was working with state regulators on a research effort to reduce the need for fumigant pesticides in strawberry fields.

Only one strawberry farmer in California used methyl iodide in 2011.

Environmental and labor organizations welcomed the company's decision.

"This is a tremendous victory for scientific integrity in the face of corporate pressure, especially for rural communities and farmworkers," said Paul Towers, a spokesman for Pesticide Action Network, a nonprofit environmental group.

The organization was one of 17 that sued Arysta LifeScience and state regulators in Alameda County Superior Court in early 2011, charging that it had failed to properly review the pesticide before approval. While a ruling was expected soon, it is unclear how the company's decision to remove the chemical from the market will affect the case.

Methyl iodide was developed to replace methyl bromide, a widely used soil fumigant banned under an international climate treaty after it was found to deplete ozone.

Arysta LifeScience said it would keep Midas registered with the federal Environmental Protection Agency, allowing for a possible reintroduction to the United States market in the future. The chemical is also registered in seven other countries, including Mexico and New Zealand. Japan is the only other country actively using it to fumigate soil.

[Return to top] *Topic Area: Public Health & Healthcare*

Daily Human Trafficking Report - 22 Mar 12

Download file

[Return to top] *Topic Area: Daily DHS Human Trafficking and Smuggling Report*

Daily Terrorism Report - 22 Mar 12

Download file

[Return to top] *Topic Area: Daily DHS Terrorism Report*

Daily Cyber Report - 22 Mar 12

Download file

[Return to top] *Topic Area: Daily DHS Cyber Report*

Daily Infrastructure Report - 22 Mar 12

Download file

UNCLASSIFIED